MINISTÉRIO DA EDUCAÇÃO
Universidade Federal de Ouro Preto
Escola de Direito, Turismo e Museologia
Curso de Graduação em Direito

Matheus Cordeiro de Barros Mendes

O papel prático do Encarregado pelo Tratamento de Dados Pessoais na dosimetria de sanções administrativas

Ouro Preto
2023

O papel prático do Encarregado pelo Tratamento de Dados Pessoais na dosimetria de sanções administrativas

Matheus Cordeiro de Barros Mendes

Trabalho Final de Curso apresentado como parte dos requisitos para obtenção do Grau de Direito na Universidade Federal de Ouro Preto.

Área de concentração: Proteção de dados, LGPD.
Orientador: Professor Roberto Porto Nogueira – UFOP
Coorientadora: Kelly Christine Oliveira Mota de Andrade - UFOP

Ouro Preto
2023

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Matheus Cordeiro de Barros Mendes

O papel prático do Encarregado pelo Tratamento de Dados Pessoais na dosimetria de sanções administrativas

Monografia apresentada ao Curso de Direito da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Direito

Aprovada em 30 de agosto de 2023;

Membros da banca:

Dr. Roberto Henrique Pôrto Nogueira - Orientador(a) (UFOP)
Kelly Christine Oliveira Mota de Andrade - Coorientadora (Mestranda PPGD UFOP)
Dra. Renata BArbosa de Almeida - Avaliadora - (UFOP)
Jéssyca Caroliny Fernandes Araújo - Avaliadora - (Mestranda PPGD UFOP)

Dr. Roberto Henrique Pôrto Nogueira, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 30/08/2023

Documento assinado eletronicamente por **Roberto Henrique Porto Nogueira**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 30/08/2023, às 19:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0583556** e o código CRC **CAC0FC65**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3559-1545 - www.ufop.br

AGRADECIMENTOS

Agradeço sinceramente ao meu orientador, professor Roberto Porto Nogueira, por sua orientação perspicaz, paciência e apoio inabalável ao longo deste projeto. sua sabedoria e encorajamento foram fundamentais para o meu desenvolvimento acadêmico e profissional.

À minha coorientadora, Kelly Christine Oliveira Mota de Andrade, expresso minha profunda gratidão por sua orientação meticulosa e comprometimento com a excelência, sua contribuição enriqueceu imensamente este trabalho.

À minha família, expresso minha mais profunda gratidão e amor. O apoio, compreensão e encorajamento constantes que vocês me proporcionaram foram a base sólida sobre a qual pude construir este trabalho. A dedicação e os valores que vocês me ensinaram foram a inspiração que me guiou em cada etapa deste caminho. A todos os membros da minha família, meu sincero obrigado.

E à Universidade Federal de Ouro Preto, estendo meus agradecimentos pela oportunidade de estudar em uma instituição de renome, pelo ambiente propício à pesquisa e pelo suporte contínuo que permitiu a realização deste trabalho.

A todos, minha eterna gratidão.

RESUMO

A Lei Geral de Proteção de Dados (LGPD), que regula o tratamento de dados pessoais no Brasil, tem se mostrado relevante perante a garantia de direitos fundamentais de liberdade e privacidade. Nesse contexto, o papel do Encarregado de Proteção de Dados (*data protection officer* - DPO) na dosimetria das sanções administrativas da lei brasileira, tema desta monografia, é oportuno, pois essa figura se identifica como central na estrutura de governança da LGPD, sendo responsável por contribuir para a conformidade das organizações com a lei, atuando como um ponto de contato entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), além de auxiliar na implementação de políticas correlatas. Afinal, insta aferir a relação entre o desempenho de tais funções e a sua aptidão para mitigar responsabilidades e prejuízos. Diante desse contexto, por meio de um estudo jurídico-dogmático que lança mão, especialmente, de fontes literárias, alcança-se a importante conclusão de que o processo de dosimetria das sanções administrativas na LGPD perpassa pela adoção de boas práticas e de uma estrutura de governança aptas a atenuarem riscos e prejuízos ligados a violações da lei. A análise da atuação do encarregado é útil, portanto, para a compreensão de seu papel nas práticas organizacionais de tratamento de dados, especialmente no que respeita aos atributos de seu papel e as repercussões de sua atuação para a dosimetria de sanções administrativas. O estudo aborda os mecanismos a serem utilizados pelo encarregado, realçando que a adoção de boas práticas e uma estrutura de governança adequada são essenciais. Os resultados indicam que uma atuação eficaz pode minimizar riscos e prejuízos associados às violações da normativa brasileira, e que a compreensão precisa das responsabilidades do encarregado revela-se relevante para a implementação de políticas de proteção de dados e para a dosimetria de sanções administrativas

Palavras-chave: Boas práticas; Dosimetria; Encarregado; Governança de dados; LGPD.

ABSTRACT

The General Data Protection Law (LGPD), which regulates the treatment of personal data in Brazil, has proven to be relevant in guaranteeing fundamental rights of freedom and privacy. In this context, the role of the Data Protection Officer (DPO) in the dosimetry of administrative sanctions under Brazilian law, the subject of this monograph, is timely, as this figure is identified as central in the governance structure of the LGPD, being responsible for contributing to organizations' compliance with the law, acting as a point of contact between the organization, data subjects, and the National Data Protection Authority (ANPD), as well as assisting in the implementation of related policies. Ultimately, it is necessary to assess the relationship between the performance of such functions and their ability to mitigate responsibilities and damages. In light of this context, through a juridical-dogmatic study that relies, especially, on literary sources, the important conclusion is reached that the process of dosimetry of administrative sanctions in the LGPD is permeated by the adoption of good practices and a governance structure capable of mitigating risks and damages related to violations of the law. The analysis of the DPO's performance is useful, therefore, for understanding their role in organizational data treatment practices, especially with regard to the attributes of their role and the repercussions of their actions for the dosimetry of administrative sanctions. The study addresses the mechanisms to be used by the DPO, highlighting that the adoption of good practices and an adequate governance structure are essential. The results indicate that effective action can minimize risks and damages associated with violations of Brazilian regulations, and that a precise understanding of the DPO's responsibilities proves to be relevant for the implementation of data protection policies and for the dosimetry of administrative sanctions.

Keywords: Data Governance; Dosimetry; Data Protection Officer; Good Practices; LGPD.

SUMÁRIO

1 Introdução 1

2 O Encarregado de Proteção de Dados 4

2.1 Contexto da LGPD 5

2.2 Princípios da LGPD 6

2.3 Tratamento de dados e seus agentes 10

2.4 Autoridade Nacional de Proteção de Dados 15

2.5 Definição do encarregado 16

2.5.1 Obrigatoriedade para nomeação de encarregado 18

2.6 Atribuições e Responsabilidades do encarregado 20

2.6.1 Monitoramento do Cumprimento da LGPD 20

2.6.2 Canal de Comunicação com a ANPD e os Titulares de Dados 21

2.7 Desafios e Melhores Práticas para o encarregado 21

2.7.1 Melhores Práticas para o encarregado 22

2.8 Conclusão 25

3 A Implementação De Ferramentas De Boas Práticas E Governança NA Lgpd 26

3.1 Uso de *Compliance* na LGPD 26

3.2 *Privacy by design* 29

3.3 Implementação de boas práticas 31

3.4 Governança de dados 34

3.5 *Accountability* 35

3.6 Relatório de Impacto à Proteção de Dados (RIPD) 37

3.7 Responsabilidade no contexto da LGPD 39

4 Processo De Dosimetria De Sanções Administrativas Na Lgpd 43

4.1 Parâmetros legais para as sanções administrativas 44

4.2 O Processo de Dosimetria das Sanções Administrativas na LGPD ...45

4.3 O Primeiro Caso de Multa por Descumprimento à LGPD 47

4.4 O Papel do DPO na Dosimetria de Sanções.....48

4.5 A Resolução Cd/Anpd Nº 4, De 24 De Fevereiro De 2023.....49

5 Conclusão 54

Referências.....56

1 INTRODUÇÃO

A era digital traz consigo uma quantidade significativa de dados pessoais, que são tratados em todo o mundo. Esse cenário levanta preocupações sobre a privacidade e a segurança dos dados pessoais dos indivíduos. (LUCAS e FÉLIX, 2022, p. 8). A crescente conscientização sobre essas questões resulta na promulgação de leis e regulamentações específicas para proteger os direitos dos titulares no que diz respeito ao tratamento de seus dados pessoais.

Reconhecendo essas mudanças, o Brasil promulga a Lei n°13.709, de 14 de agosto de 2018, LGPD, com o objetivo de criar um quadro regulatório para a proteção de dados pessoais. A lei, que é amplamente inspirada na Regulamentação Geral de Proteção de Dados da União Europeia (GDPR), apresenta noções jurídicas correlatas, dentre os quais ganha destaque a figura do Data Protection Officer (DPO) que, no Brasil, aproxima-se do sujeito intitulado encarregado pelo tratamento de dados pessoais.

O encarregado pela proteção de dados é a figura no contexto da lei brasileira que tem a responsabilidade de garantir se respeite a proteção de dados pessoais em suas atividades cotidianas (BRASIL, 2018). Seus deveres, competências e responsabilidades, definidos em lei, desafiam a adequado entendimento do papel prático desse sujeito na conjuntura respectiva, em especial na dosimetria das sanções administrativas previstas na LGPD.

A lei brasileira possui um alcance extenso e impacta praticamente todos os setores da economia. As entidades públicas e privadas que coletam, processam ou armazenam dados pessoais são obrigadas a cumprir uma série de requisitos para garantir que os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural sejam respeitados. Não surpreende, portanto, que a sua implementação efetiva seja um desafio considerável para os agentes de tratamento.

Um aspecto particularmente desafiador da LGPD é a dosimetria de sanções administrativas. Essa normativa estabelece uma variedade de sanções que a Autoridade Nacional de Proteção de Dados (ANPD) pode impor aos agentes de tratamento que não cumprem os requisitos para tanto. (BRASIL, 2018). Essas

sanções podem variar desde advertências até multas substanciais e proibições de processamento de dados. A determinação de qual sanção é apropriada em um determinado caso - a dosimetria - é uma tarefa complexa que requer uma consideração cuidadosa de fatores, incluindo a gravidade da violação, a quantidade de pessoas afetadas, o nível de negligência ou intenção do infrator e as medidas tomadas para mitigar o dano.

Neste contexto, o encarregado tem um papel relevante, pois como o profissional que serve de elo comunicativo entre diferentes partes interessadas, tem a oportunidade e a responsabilidade de influenciar a dosimetria das sanções. No entanto, cabe registrar a imprecisão das definições legais acerca do papel prático do encarregado na dosimetria das sanções administrativas. E mais: há uma falta de literatura acadêmica sobre o assunto, pois muitos dos estudos existentes se concentram em aspectos mais gerais da proteção de dados.

Diante da importância da LGPD e da necessidade de sua efetiva implementação, é fundamental compreender o papel prático do encarregado no processo de dosimetria de sanções administrativas previstas na lei brasileira. Esse é o objetivo geral do presente trabalho. Para tanto, vale compreender o contexto e os fundamentos da LGPD, assim como suas implicações para as organizações que tratam dados pessoais; investigar as atribuições e as responsabilidades do encarregado no âmbito da lei brasileira; examinar o processo de dosimetria de sanções administrativas estabelecido pela ANPD; identificar as melhores práticas e estratégias adotadas pelos encarregados para prevenir violações e garantir o cumprimento da LGPD.

Para a realização da monografia, adota-se uma abordagem metodológica baseada em pesquisa bibliográfica e documental. A pesquisa bibliográfica envolve a revisão de literatura acadêmica. A pesquisa documental, por sua vez, diz respeito à análise de documentos legais e regulatórios relacionados à proteção de dados pessoais no Brasil, incluindo a LGPD e as resoluções e orientações editadas pela ANPD. Oportunamente, pode ter lugar a abordagem de casos práticos de aplicação de sanções administrativas pelo órgão, a fim de ilustrar a dosimetria em sua dimensão prática.

O trabalho está organizado em cinco capítulos. Além da introdução, o segundo capítulo apresenta uma revisão da literatura sobre a figura do Encarregado, de modo a explorar aspectos centrais. O terceiro capítulo discute os deveres do encarregado, suas atribuições e responsabilidades no contexto da LGPD. Seguindo, o quarto capítulo enfrenta o processo de dosimetria de sanções administrativas previsto na lei brasileira, analisando as etapas, os critérios e as sanções aplicáveis. Por fim, o quinto capítulo apresenta as considerações finais do estudo.

Espera-se que este estudo contribua para o entendimento e a disseminação do conhecimento sobre o papel prático do Encarregado na dosimetria de sanções administrativas previstas na LGPD, oferecendo suporte técnico para a implementação efetiva da lei, com a proteção adequada dos dados pessoais.

2 O ENCARREGADO DE PROTEÇÃO DE DADOS

A proteção de dados pessoais, em nossa sociedade contemporânea, adquiriu uma importância inegável. A era digital, caracterizada pela circulação massiva de informações, trouxe consigo uma coleta, armazenamento e processamento colossal de dados pessoais por organizações globais (MALDONADO e BLUM, 2019).

A LGPD, conforme mencionado por Silveira (2020), é um marco legal que reflete essa importância. Fundamentada na Constituição Federal, especificamente no princípio da dignidade da pessoa humana art. 1º, III (BRASIL, 1988), a LGPD é um reflexo da necessidade de proteção dos dados pessoais em nossa sociedade.

Silveira (2020) destaca a potencialidade lesiva do tratamento indevido de dados pessoais, sobretudo à luz das recentes transformações tecnológicas. As inovações tecnológicas, apesar de seus inúmeros benefícios, ampliaram exponencialmente os riscos associados à violação da privacidade e à proteção de dados (FONTES e LÜTGE, 2021)

A proteção de dados no Brasil, portanto, não é apenas uma questão de conformidade legal, mas também uma questão de responsabilidade social e ética. (MALDONADO e BLUM, 2019) . Nesse contexto, a figura do encarregado ganha ainda mais relevância.

A LGPD, em seu Art. 5º, I (2018), apresenta uma definição ampla de dados pessoais, abrangendo qualquer informação que possa identificar uma pessoa. A lei também reconhece a existência de "dados pessoais sensíveis" Art. 5º, II, (2018), que revelam aspectos sensíveis da vida de uma pessoa, como dados de saúde de um paciente, salários entre outros, e de dados anonimizados Art. 5º, III, (2018), que se referem a um titular que não pode ser identificado.

Nesse contexto de dados pessoais, é possível estabelecer uma percepção sobre a profundidade e a importância da proteção dessas informações. A compreensão de Machado (2018) permite entender que a proteção de dados pessoais não é apenas uma questão de privacidade, mas também de segurança, dignidade e autonomia dos indivíduos.

Portanto, é com essa compreensão ampliada que devemos abordar o próximo tópico de nossa discussão: a LGPD e seu papel no cenário brasileiro. A lei brasileira

surge como uma resposta a esse cenário complexo e multifacetado, buscando estabelecer diretrizes claras e eficazes para a proteção de dados pessoais no Brasil.

2.1 Contexto da LGPD

A análise histórica da proteção de dados pessoais, como apontado por Cascaes (2019), revela que a preocupação com essa questão remonta ao século XX, com a Declaração Universal dos Direitos Humanos da ONU já sinalizando a necessidade de proteger a privacidade dos cidadãos. A consolidação dessa proteção, no entanto, ocorreu apenas na década de 1980, com a Convenção 108, que estabeleceu diretrizes para o respeito aos direitos e liberdades fundamentais no contexto do tratamento automatizado de dados pessoais (CASCAES, 2019).

A Convenção 108, formalmente conhecida como "Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados Pessoais", foi um marco na proteção de dados pessoais, estabelecendo princípios fundamentais para o tratamento desses dados. Aberta para assinatura pelo Conselho da Europa em 1981, delineou princípios-chave como a qualidade dos dados, a segurança, a finalidade da coleta, e os direitos dos indivíduos cujos dados são coletados, servindo como base para muitas leis nacionais de proteção de dados. (BRANCHER, 2022)

Cascaes (2019) também destaca que, com o advento das tecnologias digitais e o compartilhamento global de dados, tornou-se necessário revisar e atualizar as diretrizes existentes. Isso levou à criação do Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679), que expandiu o âmbito de aplicação da proteção de dados, permitindo sua aplicabilidade além das fronteiras da União Europeia. No Brasil, essa necessidade de um regulamento mais detalhado e específico resultou na aprovação da LGPD em 2018.

A LGPD é um marco legal que reflete a necessidade crescente de proteger a privacidade e os dados pessoais em um mundo cada vez mais digitalizado. Maldonado e Blum (2019) destacam que a LGPD e a GDPR, surgiram como respostas à necessidade de proteção legal dos direitos fundamentais, como a privacidade, em face da quantidade avassaladora de dados coletados na era digital.

A promulgação da LGPD foi um passo importante do Brasil rumo à construção de uma “sociedade digital” (MALDONADO e BLUM, 2019). Os autores descrevem a LGPD como um grande pacto social que, ao impor alguns limites precisos, pacifica campos de conflito de modo a cimentar a confiança necessária para o desenvolvimento de longo prazo.

No entanto, Fernandes (2022) identifica que, apesar da crescente conscientização sobre a importância da proteção de dados pessoais no Brasil, ainda há um longo caminho a ser percorrido para a plena compreensão e implementação da LGPD nas organizações.

A partir dessas constatações, torna-se evidente a necessidade de entender os princípios que norteiam a lei brasileira. Nesse sentido, o próximo tópico irá abordar os princípios que são aplicáveis no tratamento de dados na LGPD.

2.2 Princípios da LGPD

No contexto da lei de proteção de dados brasileira, é fundamental destacar que esta é uma legislação principiológica (2020). Como tal, seus dispositivos devem ser interpretados e aplicados em harmonia com os princípios constitucionais e direitos fundamentais, bem como com outras legislações que abordam temas correlatos à proteção de dados pessoais (ALMEIDA, 2020, p. 158-159)

A LGPD é fundamentada em direitos de natureza constitucional, como o direito à privacidade e à liberdade (BRASIL, 2018). Estes direitos são concretizados na noção de autodeterminação informativa, que é um dos fundamentos da lei brasileira. Este princípio fornece ao titular dos dados uma série de instrumentos e meios de tutela para efetivar suas escolhas em relação ao uso de seus dados pessoais (ALMEIDA, 2020, p. 179).

Os princípios da LGPD são fundamentais para orientar a interpretação e aplicação da legislação. Segundo seu artigo 6º, as atividades de tratamento de dados devem ser regidas pelos seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação, e responsabilização e prestação de contas. (BRASIL, 2018)

O princípio da finalidade, por exemplo, determina que o tratamento de dados pessoais deve ser realizado para “propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.” (BRASIL, 2018) Lima (2020) enfatiza que este princípio é essencial para garantir a transparência e a responsabilidade no tratamento de dados pessoais. Ele serve como uma garantia para o titular dos dados, assegurando que seus dados pessoais serão utilizados de maneira responsável e de acordo com as finalidades previamente estabelecidas.

Já o princípio da necessidade restringe o tratamento de dados ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. (BRASIL, 2018) O princípio da necessidade, conforme discutido por Maldonado e Blum (2019), é um dos pilares fundamentais da LGPD. Esse princípio está intrinsecamente ligado aos princípios da finalidade e da adequação, pois enfatiza a delimitação da licitude do tratamento de dados pessoais de acordo com a sua finalidade. A característica principal do princípio da necessidade é a limitação do tratamento ao mínimo necessário para se atingir a finalidade pretendida, conhecido como "minimização de dados" (MALDONADO e BLUM, 2019). Isso envolve uma avaliação de quais espécies de dados são realmente imprescindíveis, ou seja, dados pertinentes e não excessivos.

Em seguida, em análise ainda do art. 6 (BRASIL, 2018), temos o princípio do livre acesso, garante ao titular o direito de “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”. Almeida (2020) destaca que a LGPD impõe uma série de deveres aos agentes de tratamento para garantir a operacionalização deste direito. Isso inclui a necessidade de manter um registro das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse. O autor identifica assim, uma responsabilidade das organizações em documentar suas atividades de tratamento de dados e estar preparadas para justificar suas ações.

O legítimo interesse é um conceito jurídico que se refere a uma base legal para o tratamento de dados pessoais. De acordo com o artigo 7º, inciso IX (BRASIL, 2018), esse conceito deve servir como base do controlador ou de terceiros como fundamento

para o tratamento de dados pessoais, desde que não viole os direitos e as liberdades fundamentais do titular, nem a sua privacidade e autodeterminação informativa (art. 2º, I e II).

No contexto da mesma normativa, o art.10 (BRASIL, 2018) estabelece parâmetros para a aplicação do legítimo interesse, exigindo que o controlador tenha finalidades legítimas e situações concretas que devem ser analisadas individualmente para confirmar sua aplicação. O legítimo interesse pode ser visto como uma alternativa responsável para o uso de dados, com potencial para desenvolvimento econômico e inovação, garantindo o direito à privacidade dos titulares.

Retornando à análise principiológica, o princípio da transparência, pode ser considerado um dos mais relevantes para a atuação do encarregado, pois exige que as informações sobre o tratamento de dados sejam claras, adequadas e ostensivas, garantindo ao titular o direito de fácil acesso às informações sobre o tratamento de seus dados (LIMA, 2020). A transparência segundo Maldonado e Blum (2019) é vista como um meio de inspirar credibilidade no titular dos dados em relação ao ente público controlador dos dados, estabelecendo uma relação clara com o princípio da responsabilidade e prestação de contas. Os autores ainda pontuam que este princípio visa garantir que o titular dos dados tenha conhecimento de quem é o agente do tratamento e sobre quais fundamentos irá ocorrer o devido tratamento de dados.

Segundo Almeida (2020), outro princípio contexto da LGPD, é o princípio da qualidade dos dados, cujo autor identifica como fundamental para garantir que as decisões tomadas com base nesses dados sejam assertivas e representem corretamente o titular, evitando decisões equivocadas devido a um banco de dados desatualizado.

Consecutivo a isso, o princípio do livre acesso, segundo, Maldonado e Blum (2019) é um dos pilares da LGPD. É um princípio que garante que os titulares dos dados tenham acesso facilitado às informações sobre o processamento de seus dados, incluindo a finalidade específica do processamento, a duração, a identidade do controlador, as informações sobre o uso compartilhado de dados e as responsabilidades dos agentes que realizarão o tratamento. O livre acesso é um direito fundamental que permite ao titular ter controle sobre seus próprios dados e tomar decisões informadas sobre como eles são usados.

Em conexão com o livre acesso, o princípio da segurança é outro aspecto crucial da LGPD. Ele exige que medidas técnicas e administrativas sejam adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018). A segurança dos dados é uma responsabilidade compartilhada entre o controlador e o operador dos dados, e ambos devem tomar medidas para garantir que os dados sejam tratados de maneira segura e protegida. (MALDONADO e BLUM, 2019)

Ao identificar os agentes de tratamento denominados controlador e operador na LGPD, compreende-se que o controlador é caracterizado como a entidade, seja ela pessoa física ou jurídica, encarregada de estabelecer as decisões relativas ao tratamento de informações pessoais. De acordo com o disposto no artigo 5º, inciso VI (BRASIL, 2018), o controlador é incumbido de definir as finalidades e os métodos de tratamento, atuando em consonância com a legislação vigente e garantindo a salvaguarda dos direitos dos titulares dos dados.

O operador, por outro lado, é a entidade que realiza o tratamento de dados pessoais em nome do controlador. De acordo com o artigo 5º, inciso VII (BRASIL, 2018), o operador atua seguindo as instruções fornecidas pelo controlador, com a responsabilidade de cumprir os objetivos definidos e os requisitos legais, garantindo assim a conformidade com a lei e a proteção dos dados pessoais.

Avançando na análise dos princípios que regem a LGPD, destaca-se o princípio da prevenção que orienta que o controlador e o operador devem adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (BRASIL, 2018). Isso significa que as organizações devem ser proativas na proteção dos dados pessoais, adotando medidas preventivas para evitar violações de dados e outros danos potenciais.

Nesse mesmo sentido, o art.6 da lei, cita o princípio da não discriminação que proíbe o tratamento de dados para fins discriminatórios ilícitos ou abusivos (BRASIL, 2018). Sendo uma clara maneira, de expor, que os dados não devem ser usados de uma maneira que resulte em discriminação contra o titular dos dados. Um princípio é particularmente relevante no contexto de decisões automatizadas e perfis, onde há

um risco de discriminação com base em características pessoais. (MALDONADO e BLUM, 2019)

Segundo o último princípio estabelecido na lei, o da responsabilização e prestação de contas, exigi que o agente demonstre a “adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas” (BRASIL, 2018). Este princípio exige que o agente de tratamento de dados (seja controlador ou operador) não apenas adote medidas eficazes para garantir a conformidade com as normas de proteção de dados pessoais, mas também seja capaz de comprovar essa conformidade. Em outras palavras, não basta simplesmente seguir as regras; o agente deve também ser capaz de demonstrar e documentar que as medidas tomadas são eficazes na proteção dos dados pessoais.

A ênfase na comprovação da eficácia dessas medidas reflete uma abordagem proativa e transparente à proteção de dados, garantindo que os direitos dos titulares dos dados sejam respeitados e que as organizações sejam responsáveis por suas práticas de tratamento de dados. Isso reforça a confiança na gestão de dados e promove uma cultura de responsabilidade e conformidade dentro das organizações que lidam com informações pessoais.

Após a explanação dos princípios da LGPD, estamos aptos a adentrar na análise dos agentes de tratamento dentro do contexto desta lei. O objetivo é identificar suas características e particularidades, conforme destacado na literatura especializada, que os reconhece como elementos fundamentais para uma compreensão adequada do tema em questão.

2.3 Tratamento de dados e seus agentes

Para uma compreensão adequada do contexto no qual o encarregado se insere, é importante examinar inicialmente o termo tratamento de dados e os agentes que realizam esse tipo de operação. Este artigo, portanto, antes de se aprofundar especificamente na figura do encarregado, propõe uma breve exploração do tratamento e seus agentes, cuja presença é fundamental para a compreensão do tema.

Na LGPD, a definição de tratamento de dados está no art. 2. ° da lei, cujo “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.” (BRASIL, 2018).

Além dessa definição, a lei brasileira indica de forma expressa alguns requisitos para o correto tratamento de dados, que pode acontecer, da forma como veremos a seguir, segundo o art. 7° da LGPD:

> I – mediante o fornecimento de consentimento pelo titular;
> II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018)

Esse artigo, fornece uma base sólida para o tratamento de dados ocorrer sob condições legais. Um fator a ser destacado, é o consentimento realizado nessa operação, o consentimento é definido no Art. 5º, Inciso XII (BRASIL, 2018) como uma “manifestação livre, informada e inequívoca” pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

A lei enfatiza que o controlador deve informar ao titular a finalidade do tratamento, garantindo que o consentimento seja dado com pleno conhecimento da razão e da necessidade do uso dos dados pessoais, conforme art. 7º, I e art. 5º, XII (BRASIL, 2018). Portanto, o consentimento não é apenas uma formalidade, mas um

processo deliberado que requer transparência e responsabilidade por parte do controlador, assegurando os direitos e as liberdades fundamentais do titular dos dados.

Nesse contexto, é possível identificar o requisito consentimento, como um fator crucial para que ocorra um correto tratamento de dados, sem o mesmo, a operação de tratamento torna ilegal, pois o consentimento, como um dos pilares para o tratamento de dados pessoais, é estabelecido após a clara definição da finalidade e da necessidade do tratamento. (LIRA e MACHADO, 2022)

Sendo assim, essa breve introdução acerca do tratamento de dados é apenas o primeiro passo para desvendar a complexidade da LGPD. Agora, é essencial que nos aprofundemos nos atores que desempenham papéis fundamentais neste processo: os agentes de tratamento de dados. Esses agentes são os protagonistas na manipulação dos dados, e suas ações têm implicações diretas na proteção dos direitos dos titulares dos dados. Vamos, então, explorar quem são esses agentes, suas responsabilidades e como eles contribuem para a conformidade com a LGPD.

Os agentes de tratamento de dados, conforme definido pela LGPD, são as figuras centrais na manipulação de dados pessoais. Eles podem ser classificados, conforme art.5°, IX (2018), em duas categorias principais: o controlador e o operador.

O controlador, como exemplo, conforme definido no art. 5º, VI, da LGPD (BRASIL, 2018), é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. A lei brasileira atribui obrigações específicas ao controlador, como a elaboração de relatório de impacto à proteção de dados pessoais (RIPD), a comprovação de que o consentimento obtido do titular atende às exigências legais e a comunicação à ANPD da ocorrência de incidentes de segurança.

A elaboração do RPID é um dos requisitos estabelecido pela LGPD. Esse relatório é um documento que deve ser preparado pelo controlador e tem como objetivo avaliar os processos de tratamento de dados pessoais, identificando os riscos e as medidas, salvaguardas e mecanismos de mitigação adotados.

De acordo com o artigo 38 da LGPD (BRASIL, 2018), o controlador deve elaborar o relatório de impacto à proteção de dados pessoais, referente às operações de tratamento de dados sob sua responsabilidade, quando o tratamento resultar em

riscos às liberdades civis e aos direitos fundamentais. O relatório deve conter, no mínimo, a descrição dos processos de tratamento de dados que possam gerar riscos, a identificação dos riscos, a avaliação da necessidade e da proporcionalidade do tratamento, e a descrição das medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Em outros aspectos da lei, Leonardi (2020), identifica que o controlador que determina as finalidades e as maneiras de tratamento dos dados pessoais, ou seja, controla tanto os motivos quanto os métodos da atividade de tratamento. A caracterização como controlador é particularmente importante no contexto de transferências internacionais.

No contexto da LGPD, as transferências internacionais referem-se ao ato de enviar dados pessoais para um país estrangeiro ou organismo internacional do qual o Brasil seja membro. Essa transmissão deve ser realizada sob condições específicas para garantir que os direitos dos titulares dos dados sejam protegidos, mesmo quando os dados ultrapassam as fronteiras nacionais (BRASIL, 2018).

De acordo com o artigo 33 (BRASIL, 2018), a transferência internacional de dados pessoais é permitida em situações como quando o país de destino oferece proteção adequada aos dados; quando o controlador comprova garantias de cumprimento dos princípios da LGPD; em cooperação jurídica internacional; para proteger a vida ou a incolumidade física do titular ou de terceiro; mediante autorização da ANPD; em acordo de cooperação internacional; para execução de política pública ou atribuição legal do serviço público; com consentimento específico do titular; ou para cumprimento de obrigação legal ou contratual pelo controlador (BRASIL, 2018).

Essas condições estabelecidas pela lei brasileira visam assegurar que os dados pessoais dos titulares sejam tratados com o mesmo nível de proteção que teriam se permanecessem no Brasil. Ao definir como e por que tratar dados pessoais, o controlador deve observar quais mecanismos de transferência internacional são os mais apropriados entre aqueles disponíveis na LGPD, bem como avaliar se os operadores que utiliza no contexto de suas atividades realizam o tratamento de dados pessoais fora do país (LEONARDI, 2020).

O controlador também tem responsabilidades em relação à segurança dos dados. O art. 42 da LGPD (BRASIL, 2018) prevê a responsabilidade solidária dos

controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados (SCHREIBER, 2020). Isso significa que, mesmo quando a lesão for causada por fato imputável exclusivamente ao operador, o controlador, justamente em razão de sua posição de destaque na dinâmica do tratamento, poderá ser chamado a responder solidariamente, de modo a garantir a efetiva indenização da vítima (SCHREIBER, 2020, p. 514).

Continuando essa breve introdução sobre os agentes de tratamento de dados, é importante destacar a figura do operador. Este é outro papel crucial no ecossistema de proteção de dados, que complementa e interage com o controlador. Vamos agora explorar as responsabilidades e obrigações do operador no contexto da LGPD.

Segundo a LGPD, em seu artigo 5º. (BRASIL, 2018) define o operador como a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador". O operador, portanto, atua sob as instruções do controlador e é responsável por realizar o tratamento de dados pessoais conforme essas instruções. No entanto, este agente ainda pode ser responsabilizado por violações à LGPD, conforme os arts. 42 e 52 (BRASIL, 2018).

Em situações, cujo operador viola a legislação de proteção de dados ou não segue as instruções lícitas que lhe foram passadas pelo controlador, o operador pode ser responsabilizado diretamente pelos danos causados, conforme art.42, inciso I (BRASIL, 2018).

No entanto, mesmo quando a lesão é causada por um fato imputável exclusivamente ao operador, o controlador, devido à sua posição de destaque na dinâmica do tratamento de dados, pode ser chamado a responder solidariamente, garantindo assim a efetiva indenização da vítima (SCHREIBER, 2020).

A figura do operador, conforme discutido, desempenha um papel crucial no tratamento de dados pessoais, agindo sob as instruções do controlador e sendo responsabilizado por qualquer violação da LGPD. No entanto, a dinâmica do tratamento de dados pessoais não se limita apenas à interação entre o controlador e o operador. Há um terceiro elemento crucial nesse cenário: a Autoridade Nacional de Proteção de Dados.

A ANPD é o órgão responsável por fiscalizar e garantir a aplicação da lei brasileira de proteção de dados, além de orientar a sociedade sobre os direitos dos

titulares de dados e as obrigações dos agentes de tratamento. Vamos agora explorar mais profundamente o papel e as responsabilidades da ANPD.

2.4 Autoridade Nacional de Proteção de Dados

A ANPD, exerce um papel importante na aplicação das sanções administrativas previstas na lei brasileira. Como entidade reguladora, sua responsabilidade abrange a supervisão, orientação, fiscalização e imposição de sanções em casos de descumprimento da lei. (BRASIL, 2018)

Inicialmente, a promulgação da LGPD gerou frustrações devido aos vetos aos artigos 55 a 59 da Lei nº 13.709/18, que previam a criação da ANPD com a atribuição de fiscalizar e regulamentar a lei. Esses vetos levantaram dúvidas sobre a efetividade do diploma legal como um todo. Além disso, a ausência de uma autoridade nacional de proteção de dados no Brasil, diferentemente do que ocorreu na União Europeia com o RGPD, que contou com o protagonismo das autoridades europeias, reforçou uma visão pessimista em relação à lei brasileira. (FILHO, 2021)

Para preencher essa lacuna, foi editada a Medida Provisória nº 869, posteriormente convertida na Lei nº 13.853/2019, restabelecendo a ANPD no Brasil e inserindo os artigos 55-A a 55-L na LGPD. No entanto, esses dispositivos foram alvo de críticas, pois estabeleceram a ANPD como um órgão do governo federal, vinculado à Presidência da República, em contradição com a versão original da LGPD, que conferia à ANPD o status de autarquia especial. Essa configuração como órgão da administração direta não proporciona a autonomia técnica e decisória necessária, conforme exigido pelas normas europeias, para garantir a independência dos órgãos de controle e fiscalização da proteção de dados. (FILHO, 2021)

Recentemente, foi promulgada a Lei nº 14.460 (2022), concedendo a ANPD autonomia administrativa e financeira. Esta lei, originada da MP 1.124/2022, além de conceder à ANPD o status de autarquia de natureza especial, mantendo a estrutura organizacional e as competências, também cria um cargo comissionado de diretor-presidente, sem aumento de despesas.

A ANPD se estrutura por sua organização pelo Decreto 10.474/2020 (2020). A autarquia é composta por um Conselho Diretor, composto por cinco diretores, um

deles sendo o Diretor-Presidente. Este é assistido por uma Secretaria-Geral, uma Coordenação-Geral de Administração e uma Coordenação-Geral de Relações Internacionais e Institucionais. Como órgãos seccionais, a ANPD possui uma Corregedoria, uma Ouvidoria e uma Assessoria Jurídica. Além disso, a ANPD tem três Coordenações-Gerais: a de Normalização, a de Fiscalização e a de Tecnologia e Pesquisa. (BRASIL, 2020)

Importante pontuar também, sobre a responsabilidade que recai sobre a autarquia da de uma política nacional de proteção de dados pessoais, garantia da privacidade desses dados, fiscalização e aplicação de sanções, promoção de campanhas de informação com a população sobre as normas e as políticas públicas de proteção de dados pessoais, promoção de ações de cooperação com autoridades estrangeiras sobre esse tema, proposição de diretrizes estratégicas e elaboração de relatórios anuais de avaliação da execução da política nacional de proteção de dados. (SARLET, FERNANDES e RUARO, 2020)

A ANPD, diante das diversas reponsabilidade expostas, é possível identificar o papel central do órgão, na implementação e interpretação da LGPD. No entanto, a efetivação da proteção de dados pessoais não se restringe à atuação da ANPD. Outra figura de grande relevância nesse cenário é o encarregado, cuja definição e funções veremos a seguir.

2.5 Definição do encarregado

O encarregado de proteção de dados, é um cargo essencial na estrutura de proteção de dados de uma organização, conforme definido pela lei brasileira. Essa figura é responsável por supervisionar a conformidade com a lei, atuar como ponto de contato com os titulares dos dados e a ANPD, e garantir que os direitos dos titulares dos dados sejam respeitados. Este papel é análogo ao estabelecido pelo RGPD (2016) na Europa, em vigor desde 2016. No entanto, é importante reconhecer que, embora as funções sejam semelhantes, existem diferenças específicas em cada contexto legal, refletindo as particularidades das leis e regulamentações de proteção de dados em cada jurisdição.

Inicialmente, este segmento se propõe a examinar as distinções e especificidades inerentes aos regulamentos da União Europeia, com o objetivo de compreender como o papel do encarregado é caracterizado nesses contextos. Posteriormente, a análise se voltará para a definição precisa desta figura conforme estabelecido pela legislação brasileira.

Conforme estabelecido no Artigo 37 do RGPD (2016), a designação do encarregado de proteção de dados é mandatória para entidades públicas. A mesma obrigatoriedade se aplica a organizações privadas cujas atividades principais incluem o monitoramento regular e sistemático de indivíduos de forma extensa, ou o tratamento de categorias especiais de dados pessoais em larga escala.

O Artigo 38 do RGPD (2016), por sua vez, detalha as responsabilidades do encarregado. Este artigo estabelece que essa figura deve ser envolvida em todas as questões relativas à proteção de dados pessoais. Além disso, o encarregado deve ser fornecido com os recursos necessários para desempenhar suas funções e manter seu conhecimento especializado. Essa figura também tem a obrigação de manter a confidencialidade das informações processadas, a menos que a lei exija divulgação (UNIÃO EUROPEIA, 2016).

Já segundo o Artigo 39 do RGPD (2016) lista as tarefas do encarregado, que incluem informar e aconselhar a organização e seus funcionários sobre suas obrigações de conformidade com o RGPD e outras leis de proteção de dados da União e dos Estados-Membros. Também é responsável por monitorar a conformidade com o RGPD e com as políticas da organização em relação à proteção de dados pessoais, incluindo a atribuição de responsabilidades, treinamento de pessoal e auditorias (UNIÃO EUROPEIA, 2016).

Após a análise das definições e funções do encarregado no contexto da GPDR, é fundamental voltar nosso olhar para o cenário brasileiro. A compreensão das nuances e especificidades desta figura em outros países nos oferece uma base sólida para entender e avaliar a definição qual o seu papel no Brasil. Assim, com a perspectiva global em mente, vamos agora explorar a definição do DPO conforme estabelecido pela LGPD.

No Brasil, a figura do encarregado é definida pela normativa brasileira, como veremos a seguir. De acordo com o Artigo 5º, inciso VIII da LGPD (2018), o

Encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

O Artigo 41 (2018) estabelece que o controlador deve indicar um encarregado pelo tratamento de dados pessoais. O §1º do mesmo artigo determina que a identidade e as informações de contato do encarregado devem ser divulgadas publicamente, de preferência no site do controlador. (BRASIL, 2018)

As responsabilidades do encarregado são detalhadas no §2º do Artigo 41 (BRASIL, 2018) que incluem aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações da autoridade nacional e orientar os funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

Além disso, a ANPD pode estabelecer normas complementares sobre a definição e as atribuições do Encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme previsto no §3º do Artigo 41 da LGPD. (BRASIL, 2018)

Sendo assim, além da definição segundo conceitos normativos estabelecido para o encarregado, é igualmente importante também analisar a obrigatoriedade de sua nomeação conforme estabelecido pela LGPD. Assim, na próxima seção, discutiremos em detalhes a exigência legal de nomear um encarregado e as circunstâncias em que essa obrigação se aplica.

2.5.1 Obrigatoriedade para nomeação de encarregado

Seguindo uma análise da obrigatoriedade da nomeação de um Encarregado pelo Tratamento de Dados Pessoais, é importante destacar que a lei brasileira não estabelece critérios objetivos para tal, deixando essa tarefa a cargo da ANPD (BRUNO, 2019).

Conforme o artigo 41 (BRASIL, 2018), o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. A atividade do encarregado deve ser pública e divulgada de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador, conforme o § 3° do mesmo artigo. Tal obrigatoriedade reflete a

necessidade de garantir a transparência, a responsabilidade e a conformidade no tratamento de dados pessoais, alinhando-se às melhores práticas internacionais em matéria de proteção de dados. (BRASIL, 2018). Portanto, a decisão de nomear um Encarregado deve ser devidamente documentada, visando a demonstrar que todos os fatores relevantes foram considerados para essa decisão, em observância ao princípio da prestação de contas (BRUNO, 2019).

A documentação que justifica a decisão pode ser solicitada pela ANPD e deve ser atualizada sempre que necessário, especialmente quando a empresa lança produtos ou serviços que implicam em novos tratamentos de dados pessoais. Mesmo que a conclusão seja de que a função de Encarregado não é obrigatória, a empresa pode optar pela nomeação voluntária de um Encarregado. Nesse caso, entende-se que todas as regras aplicáveis ao Encarregado obrigatório também se aplicam ao Encarregado nomeado voluntariamente. (BRUNO, 2019)

No entanto, a Resolução CD/ANPD Nº 2 (2022), trouxe uma nova perspectiva sobre essa questão. Esta resolução, deliberada pelo órgão estabeleceu critérios para eximir os agentes de tratamento de pequeno porte da nomeação obrigatória estabelecido pela lei.

Esta Resolução (BRASIL, 2022), estabelece que os agentes de tratamento de pequeno porte não são obrigados a indicar um encarregado pelo tratamento de dados pessoais, conforme exigido no artigo 41 da LGPD Contudo, o agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados para atender o disposto no artigo 41, § 2º, I da LGPD. (BRASIL, 2022)

Portanto, a nomeação de um encarregado não é obrigatória para todos os agentes de tratamento de dados. A obrigatoriedade depende do porte do agente de tratamento e do tipo de atividades de tratamento de dados que ele realiza.

A obrigatoriedade da nomeação do encarregado, é um elemento crucial para entendermos as atribuições e responsabilidades desse profissional. A lei brasileira não apenas exige a presença desse profissional nas organizações, mas também delineia suas principais funções e responsabilidades.

Assim, a transição do tópico da obrigatoriedade da nomeação para o das atribuições e responsabilidades do encarregado é uma progressão natural, pois a lei

estabelece não apenas a necessidade desse profissional, mas também o que se espera dele em termos de garantir a conformidade com a LGPD.

2.6 Atribuições e Responsabilidades do encarregado

Uma das principais responsabilidades do encarregado é oferecer aconselhamento e orientação à organização, conforme estabelecido no art. 41, § 2º. (BRASIL, 2018) em relação às obrigações legais e às melhores práticas no tratamento de dados pessoais. Além disso, deve acompanhar as mudanças na legislação e nas regulamentações pertinentes, garantindo que a organização esteja atualizada e em conformidade com as normas aplicáveis (BRASIL, 2018).

O encarregado também deve orientar a organização sobre a implementação de medidas técnicas e organizacionais adequadas para garantir a proteção dos dados pessoais. Isso inclui a definição de políticas de segurança, a realização de avaliações de impacto à proteção de dados e a criação de programas de treinamento para os funcionários (GARRIDO, 2023).

2.6.1 Monitoramento do Cumprimento da LGPD

A figura do encarregado é responsável por monitorar o cumprimento das disposições da LGPD dentro da organização. Isso envolve a realização de auditorias internas para avaliar a conformidade, a revisão de políticas e procedimentos existentes e a identificação de possíveis riscos e vulnerabilidades relacionados à proteção de dados (BRASIL, 2018).

Além disso, é possível identificar que o encarregado de proteção de dados deve trabalhar em estreita colaboração com as áreas responsáveis pelo tratamento de dados pessoais, garantindo que todas as atividades estejam em conformidade com as normas estabelecidas pela LGPD. Ademais, este profissional deve realizar análises de impacto à proteção de dados em casos em que o tratamento de dados possa representar um alto risco para os direitos e liberdades dos titulares (TEIXEIRA e GUERREIRO, 2022).

2.6.2 Canal de Comunicação com a ANPD e os Titulares de Dados

O encarregado atua como um canal de comunicação entre a organização, a ANPD e os titulares de dados. (2018) A figura do encarregado é responsável por receber e responder às solicitações dos titulares, garantindo que seus direitos sejam respeitados e que suas reclamações sejam tratadas de forma adequada (BRASIL, 2018).

O artigo 41 (BRASIL, 2018) estabelece a figura do encarregado, como o responsável por esse canal de comunicação. O encarregado atua como um intermediário entre o controlador (a entidade que determina como os dados pessoais são processados), os titulares dos dados (as pessoas cujos dados estão sendo processados) e a ANPD (a autoridade reguladora).

A nomeação de um encarregado e a criação de um canal de comunicação claro e acessível são obrigatórias para todas as organizações sujeitas à LGPD. O § 3° do artigo 41 enfatiza que a atividade do encarregado deve ser pública e divulgada de forma clara e objetiva, preferencialmente no site eletrônico do controlador (BRASIL, 2018).

Esse canal de comunicação tem várias funções importantes. Ele permite que os titulares dos dados exerçam seus direitos sob a LGPD, como o acesso, correção e exclusão de seus dados (BRASIL, 2018). Também facilita a supervisão e a aplicação da lei pela ANPD, permitindo que a autoridade reguladora se comunique efetivamente com as organizações para garantir que estejam em conformidade com a LGPD.

Além disso, o encarregado é o ponto de contato com a ANPD, responsável por representar a organização perante a autoridade reguladora. O encarregado deve cooperar com a ANPD em questões relacionadas ao tratamento de dados pessoais, fornecendo informações e documentos solicitados pela autoridade (BRASIL, 1988).

2.7 Desafios e Melhores Práticas para o encarregado

A figura do Encarregado, enfrenta uma série de desafios complexos em sua função. Como exemplo, o conflito de interesses é uma questão crítica. O encarregado, ao monitorar a conformidade das atividades de tratamento de dados pessoais, pode

encontrar-se em uma posição delicada se também for responsável por uma atividade de tratamento de dados pessoais. Bruno (2019) relaciona essa possibilidade de ter que monitorar a própria atividade, e identifica que isso pode gerar um conflito de interesses, tornando essencial a separação dessas funções.

Contudo, além do conflito de interesses, a independência do encarregado é um desafio igualmente importante. O encarregado deve ter a liberdade de desempenhar suas funções sem interferências, mesmo que suas recomendações possam não ser favoráveis aos negócios da empresa. Segundo Vainzof (2020), esse aspecto reforça a necessidade de uma posição autônoma para o DPO dentro da organização.

Além disso, o encarregado deve possuir um conhecimento técnico sólido. Isso inclui um profundo entendimento da LGPD, da regulamentação setorial de proteção de dados pessoais aplicável, e da realidade das atividades desempenhadas pela empresa. Este conhecimento é crucial para a eficácia desse profissional em suas funções (VAINZOF, 2020)

Portanto, ao analisar brevemente os desafios enfrentados pelo encarregado, é possível destacar a complexidade de sua função e a necessidade de uma abordagem cuidadosa e bem informada para a nomeação e o apoio a essa posição crucial.

2.7.1 Melhores Práticas para o encarregado

Sankievicz e Pinheiro (2020) destacam a importância da adoção de uma política de boas práticas e governança, pois inclui a determinação dos tipos de informações pessoais manipuladas, as categorias de titulares cujas informações serão processadas, o motivo pelo qual essas informações estão sendo manipuladas, a maneira como são processadas, as entidades para as quais serão direcionadas e os locais para os quais são transferidas, o período pelo qual serão guardadas e armazenadas, e os detalhes da segurança para o manuseio das informações pessoais.

Conforme a visão de Sankievicz e Pinheiro (2020), a gestão de informações pessoais transcende uma tarefa simples, exigindo uma abordagem meticulosamente estruturada e planejada. Ainda segundo os autores, a implementação de uma política de boas práticas e governança não se restringe apenas à coleta e ao armazenamento

de dados. Ela engloba uma compreensão nítida e detalhada dos tipos de informações manipuladas, a identificação dos titulares dessas informações, a razão pela qual estão sendo processadas, a metodologia empregada nesse processamento, e a identificação das entidades e locais para os quais essas informações são direcionadas e transferidas. (SANKIEVCZ e PINHEIRO, 2020)

Os autores (2020) também enfatizam a importância de determinar o período de retenção dessas informações e os mecanismos de segurança empregados para protegê-las. Essa abordagem holística, segundo Sankievicz e Pinheiro (2020), não apenas garante a conformidade com as leis e regulamentos aplicáveis, mas também promove a confiança e a transparência com os titulares dos dados.

Além disso, Sérgio Alves Jr. (2020) ressalta que a implementação de um modelo de ciclo de vida de dados pessoais aderente à LGPD implica que os agentes de tratamento conheçam os dados que estão coletando e armazenando, evitando a coleta e armazenamento irracional e sem critério algum de volumes crescentes de dados pessoais. (JR, 2020)

Continuando a discussão sobre as melhores práticas do encarregado, Saavedra (2020), destaca a conexão entre as etapas do Relatório de Impacto de Proteção de Dados (RIPD) e as melhores práticas de compliance. O relatório, uma ferramenta essencial para a prestação de contas, configura-se como um processo meticuloso que delineia o tratamento de dados. Esse processo tem a função de identificar a necessidade e/ou proporcionalidade, buscando alcançar um equilíbrio harmonioso entre os riscos inerentes a esse tratamento e os direitos que ele confere.

Além disso, Saavedra (2020) ressalta sobre a utilização da ferramenta *Privacy by Design* (PbD) como uma metodologia essencial para a implementação de um correto tratamento de dados. O PbD implica que as organizações devem sempre criar produtos e serviços que, desde o início, estejam de acordo com as diretrizes de um sistema de gestão de compliance digital ou de dados, bem como das melhores práticas de Compliance de dados (SAAVEDRA, 2020).

Essas e outras práticas, quando implementadas corretamente, servem como um elemento redutor de eventual penalidade a ser imposta pela autoridade nacional de dados (SANKIEVCZ e PINHEIRO, 2020). Isto é fundamental para o presente artigo,

pois se relaciona com a proposta posterior de adentrar nos aspectos específicos de boa prática e governança, seguindo critérios de compliance.

A relação entre compliance, governança e o encarregado é serve como parâmetro para uma gestão eficaz de informações pessoais e conformidade com as regulamentações de proteção de dados, como a LGPD. Compliance refere-se ao cumprimento de leis, regulamentos, normas e políticas aplicáveis a uma organização (MALUF, 2022). No contexto da proteção de dados, isso significa aderir às leis que regem o uso, armazenamento e transferência de informações pessoais. A governança de dados, por outro lado, envolve a gestão e o controle de informações dentro de uma organização para garantir sua qualidade, segurança e eficácia (WEBER, OESTERLE e OTTO, 2009).

É possível identificar que o encarregado é seria uma figura central na interseção entre compliance e governança. Ele é responsável por garantir que a organização cumpra todas as leis e regulamentações aplicáveis, ao mesmo tempo em que supervisiona a governança de dados para garantir que as informações sejam manuseadas de maneira ética e responsável, conforme art.41 (BRASIL, 2018). O encarregado também atua como um canal de comunicação entre a organização, os titulares dos dados e as autoridades reguladoras, promovendo transparência e confiança (SANKIEVCZ e PINHEIRO, 2020).

Neste sentido, a relação entre compliance, governança e o encarregado é intrinsecamente ligada e vital para a proteção eficaz dos dados pessoais. Através da colaboração desses três elementos, as organizações podem garantir que estejam operando dentro dos limites da lei, ao mesmo tempo em que mantêm a integridade e a segurança dos dados que manuseiam. Essa abordagem holística reflete o compromisso de uma organização com a proteção e o uso responsável das informações pessoais, alinhando-se às melhores práticas internacionais em matéria de proteção de dados.

Portanto, a função do encarregado é multifacetada e crucial para garantir a conformidade com as leis de proteção de dados e para minimizar os riscos associados ao tratamento de dados pessoais.

2.8 Conclusão

Neste capítulo, foram apresentadas a definição e as atribuições do DPO no contexto da LGPD. O encarregado desempenha um papel fundamental na garantia do cumprimento das normas estabelecidas pela legislação de proteção de dados.

Além disso, foram abordadas as figuras paralelas ao encarregado, como o controlador, o operador e a ANPD, destacando suas respectivas funções e interações. Também foram discutidos os desafios enfrentados pelo encarregado e apresentadas conceitos metodológicos para as melhores práticas, estabelecidos como ferramentas a serem utilizadas pelos agentes de tratamento e pelo próprio encarregado.

Agora, o próximo capítulo desta presente investigação, seria dedicado a investigação acerca das ferramentas utilizadas pelo encarregado sob égide da LGPD. Neste capítulo, analisando os mecanismos utilizadas pelo encarregado, que estão intrinsecamente ligadas a dosimetria das sanções administrativas.

3 A IMPLEMENTAÇÃO DE FERRAMENTAS DE BOAS PRÁTICAS E GOVERNANÇA NA LGPD

Conforme brevemente apresentado, a implementação de ferramentas para a adequação de comportamentos padronizados, tanto dos agentes de tratamento, quanto do encarregado em si, serve como parâmetro para uma boa atuação tanto dos agentes de tratamento quanto do encarregado. Estes mecanismos permitem ao encarregado monitorar a conformidade com a LGPD, identificar e mitigar riscos e garantir que os direitos dos titulares dos dados sejam respeitados.

Assim, esse capítulo tem como objetivo elucidar as especificidades de boas práticas e governança, entre outras ferramentas que devem ser utilizadas pelo encarregado, para uma análise de seu papel no desenho da responsabilidade administrativa dos agentes de tratamento, de acordo com os preceitos normativos estabelecidos pela LGPD. Ao abordar este tema, pretende-se aprofundar o propósito desta pesquisa, estabelecendo uma conexão mais sólida entre o papel do encarregado e a dosimetria das sanções administrativas.

3.1 Uso de *Compliance* na LGPD

A LGPD impõe uma série de deveres no que diz respeito ao tratamento de dados pessoais, e o *compliance* surge como uma ferramenta para garantir o cumprimento dessas obrigações.

Compliance, no contexto da proteção de dados, refere-se ao cumprimento rigoroso das leis, regulamentos e normas que governam o uso, armazenamento e transferência de informações pessoais (MALUF, 2022). Isso envolve a implementação de políticas e procedimentos que garantam que os dados sejam manuseados de acordo com os requisitos legais, incluindo a LGPD no Brasil, o GDPR na Europa, e outras regulamentações aplicáveis. A conformidade com essas regulamentações é essencial para proteger a privacidade dos indivíduos, promover a confiança e evitar penalidades legais, demonstrando o compromisso da organização com a ética e a responsabilidade no manuseio de informações pessoais (WEBER, OESTERLE e OTTO, 2009).

Portanto, o compliance na LGPD envolve garantir que esses direitos sejam respeitados em todas as operações de processamento de dados.

Segundo Tepedino, Frazão e Oliva (2019), o conceito de *Compliance* pode ser interpretado como um conjunto de medidas implementadas no cenário empresarial, cujo objetivo é assegurar a conformidade da organização com as leis em vigor. Ainda segundo os autores, essas medidas têm a função de prevenir a ocorrência de transgressões ou, caso já tenha ocorrido alguma infração, facilitar o retorno imediato a um estado de normalidade e legalidade.

A implementação do compliance na LGPD requer a adoção de uma série de "medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito", conforme disposto pelo art. 46 da lei brasileira (2018). Isso pode envolver a implementação de tecnologias de segurança da informação, a criação de políticas de privacidade e a realização de treinamentos de conscientização para os funcionários.

Ao considerar a instauração de um programa interno que se alinhe às diretrizes da LGPD, o ponto de partida é a elaboração de um projeto que planeje a conformidade da organização com a referida lei. Segundo Alfonsin (2022), a estruturação de uma implementação da LGPD está de acordo com a aplicação padrão de um modelo de Compliance. No entanto, em vez de se restringir à Análise de Risco, a implementação da LGPD engloba o Mapeamento de Dados, que consiste no inventário e registro de dados, além do mapeamento dos dados da empresa (ALFONSIN, 2022). Além disso, inclui a Avaliação de Impacto à Privacidade, que discute os impactos para a privacidade de determinado produto, serviço ou atividade da empresa, e a Avaliação de Impacto à Proteção de Dados (STEINBERG, 2011).

O inventário de dados assume uma importância no contexto da lei brasileira. Trata-se de um processo meticuloso de identificação, catalogação e classificação de todos os ativos de informação relacionados a dados pessoais dentro de uma organização, conforme estabelecido no guia de elaboração de inventário de dados pessoais (BRASIL, 2023). Essa prática permite uma visão clara e abrangente dos dados, incluindo sua localização, propriedade e sensibilidade, facilitando a gestão e a conformidade com os requisitos da LGPD. O inventário de dados é mais um passo

para entender o que a organização possui em termos de informações pessoais e é essencial para a implementação de políticas de proteção de dados, garantindo que os direitos dos titulares dos dados sejam respeitados (CAVOUKIAN, 2013).

A LGPD, por seu art. 50, estabelece que os agentes de tratamento de dados devem ser capazes de demonstrar a conformidade com os princípios e regras estabelecidos pela lei, aplicando o conceito de boas práticas, que podem ser implementados de duas formas, “por meio de associações ou de forma individual pelo controlador ou operador de dados pessoais.”. (BRASIL, 2018)

Ainda em uma análise normativa pela lei brasileira, é perceptível a complexidade da aplicação dessa ferramenta ao estabelecer deveres específicos para a figura do encarregado. Esses deveres incluem a responsabilidade por supervisionar o cumprimento da lei, organizar e atuar proativamente na comunicação entre a organização, os titulares dos dados e a ANPD (BRASIL, 2018). Esse papel de orientação, exemplificado na implementação do compliance, sublinha a relevância do encarregado nesse contexto. Nessa linha, Alfonsin (2022) reconhece que a implantação de um programa de compliance transcende a mera conformidade com os artigos da LGPD. Representa, em vez disso, uma busca efetiva por uma mudança cultural, visando um programa de conformidade alinhado com os princípios estabelecidos pela normativa.

Conforme já apresentado em sua definição normativa, o encarregado é responsável por supervisionar o cumprimento da LGPD dentro da organização, atuando como um ponto de ligação entre a organização, os titulares dos dados e a ANPD (BRASIL, 2018). Suas funções incluem a orientação sobre as práticas de tratamento de dados, a resposta a solicitações dos titulares dos dados e a colaboração com o órgão regulador. O Encarregado deve promover uma cultura de conformidade, garantindo que as políticas e procedimentos estejam alinhados com os requisitos legais e éticos.

O compliance de dados, previsto na lei brasileira, envolve a adoção de uma série de ferramentas e práticas para garantir que o tratamento de dados pessoais esteja em conformidade com a lei. Isso inclui a implementação de políticas de privacidade claras, a realização de avaliações de risco, o treinamento de pessoal, o monitoramento contínuo e a resposta a incidentes de segurança (CAVOUKIAN, 2013).

A implementação eficaz do compliance de dados requer uma abordagem integrada e proativa, envolvendo todos os níveis da organização, e deve ser adaptada às necessidades específicas e aos riscos associados ao tratamento de dados da organização.

Assim, mediante a avaliação realizada, torna-se evidente a relevância deste instrumento para todos os atores envolvidos no panorama da proteção de dados. No próximo segmento, o capítulo explora implementação do mecanismo de boas práticas, que também contribui para este processo de conformidade.

3.2 *Privacy by design*

O princípio do PbD, conforme discutido por Bioni (2021) , é uma abordagem que estabelece a privacidade e a proteção de dados como elementos intrínsecos a todo o ciclo de vida das tecnologias, desde a sua concepção inicial até a sua introdução no mercado. Ainda segundo o autor, um dos pontos chave para o entendimento do PbD é que as organizações devem criar produtos e serviços que, desde o início, estejam em conformidade com as diretrizes de um sistema de gestão de compliance digital ou de dados. Além disso, as melhores práticas de Compliance de dados devem ser aplicadas diretamente nas tecnologias, nos sistemas e nas práticas vinculadas a todo o ciclo de vida dos produtos e serviços das organizações e empresas. (BIONI, 2021)

O artigo 46 menciona que os:

> “agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”. (BRASIL, 2018)

Este artigo estabelece a obrigação dos agentes de tratamento de dados em implementar medidas de segurança adequadas, tanto técnicas quanto administrativas, para salvaguardar os dados pessoais (BRASIL, 2018). Em essência, o artigo enfatiza a necessidade de uma gestão responsável e segura dos dados

pessoais, garantindo que sejam tratados de maneira apropriada e em conformidade com a lei.

O §2º do mesmo artigo reforça a necessidade de observar essas medidas desde a “fase de concepção do produto ou do serviço até a sua execução” (BRASIL, 2018). Essa disposição legal está em consonância com o princípio do PbD, que preconiza que a privacidade e a proteção de dados devem ser consideradas desde o início do desenvolvimento de um produto ou serviço, estando integradas em todo o seu ciclo de vida.

Dessa forma, é possível identificar que o PdB pode ser um componente essencial na estruturação de sistemas de informação, especialmente no contexto da LGPD. Este princípio, conforme discutido por Bruno Bioni (2021), busca fornecer ao usuário ferramentas que promovam confiança na rede e tranquilidade quanto ao uso correto de seu consentimento.

A metodologia PbD, como Jonas Valente (2018) ressalta, fundamenta-se no reconhecimento de que a privacidade não pode ser satisfatoriamente tutelada apenas pelas estruturas regulatórias tradicionais. É necessário que a privacidade esteja enraizada na metodologia de operações das organizações (VALENTE, 2018)

Ann Cavoukian (2013) aponta os sete pilares norteadores da concepção do PbD, que incluem medidas proativas e preventivas, privacidade como padrão, privacidade inserida no design, funcionalidade completa, segurança de ponta a ponta, visibilidade e transparência, e respeito pela privacidade do usuário.

O primeiro pilar é a "Proatividade Preventiva", que enfatiza a prevenção de invasões à privacidade antes que elas ocorram, em vez de remediar os problemas após sua ocorrência. O segundo pilar é a "Privacidade como Configuração Padrão", garantindo que os dados pessoais sejam automaticamente protegidos em qualquer sistema ou prática de negócios, sem que o indivíduo precise tomar medidas para proteger sua privacidade (CAVOUKIAN, 2013).

O terceiro pilar, "Privacidade Incorporada no Design", enfatiza a integração da privacidade desde o início do design do sistema. O quarto pilar, "Funcionalidade Total - Soma Positiva, não Zero", rejeita compromissos entre privacidade e segurança, buscando ambas. O quinto pilar, "Fim da Vida Útil dos Dados Protegidos", diz respeito à proteção de dados desde o momento da coleta até a destruição segura no final de

sua vida útil. O sexto pilar, "Visibilidade e Transparência", garante que todas as partes interessadas estejam cientes de como os dados são gerenciados e protegidos. Finalmente, o sétimo pilar, "Respeito pela Privacidade do Usuário", enfatiza o respeito pelos interesses dos usuários, incluindo a garantia de precisão, qualidade e acessibilidade aos próprios dados pessoais (CAVOUKIAN, 2013).

O encarregado, ao adotar os princípios do PbD, pode garantir que a privacidade seja integrada em todos os aspectos do processamento de dados, desde o início (CAVOUKIAN, 2013).

O papel do encarregado na LGPD inclui não apenas a supervisão da conformidade, mas também a promoção de uma cultura de proteção de dados dentro da organização. Isso envolve a implementação de políticas e práticas que refletem os sete pilares do PbD. Por exemplo, o encarregado pode garantir que a privacidade seja a configuração padrão em todos os sistemas (segundo pilar) e que haja transparência e responsabilidade em relação ao processamento de dados (sexto pilar). Essa abordagem proativa e centrada no design ajuda a organização a cumprir suas obrigações legais sob a LGPD e fortalece a confiança dos titulares dos dados na maneira como suas informações pessoais são tratadas.

A implementação do PbD, portanto, não é apenas uma questão de conformidade legal, mas também uma questão de ética e boa-fé. A arquitetura de rede responsável, correta e leal aos seus propósitos, que transmite confiança aos titulares de dados de que os controladores não se comportarão de forma contraditória e desleal ao longo da relação, será uma arquitetura que se alinha ao modelo de PbD e à cláusula geral da boa-fé objetiva, em busca de efetividade e garantias de proteção da autodeterminação informativa.

3.3 Implementação de boas práticas

Sankievicz e Pinheiro (2020) ressaltam a relevância da implementação de uma política de boas práticas e governança. Esta política engloba a identificação dos tipos de dados pessoais que serão tratados, as categorias de titulares cujos dados serão processados, a justificativa para o tratamento desses dados, a metodologia de tratamento, os destinatários dos dados e para onde serão transferidos, o período de

retenção e armazenamento dos dados, bem como os detalhes de segurança para o tratamento dos dados pessoais (2018). Essas ferramentas, implementam e auxiliam o processo de definição de qualidade desses dados contidos no tratamento realizado. (SANKIEVCZ e PINHEIRO, 2020).

Com base no Art. 50 (BRASIL, 2018), a definição de boas práticas refere-se a um conjunto de regras e procedimentos estabelecidos por controladores e operadores de dados. Essas regras de boas práticas e de governança devem estabelecer as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

A definição também enfatiza a necessidade de considerar a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular. Além disso, o controlador pode implementar um programa de governança em privacidade que demonstre comprometimento com normas e boas práticas relativas à proteção de dados pessoais, seja adaptado à estrutura da organização, estabeleça políticas e salvaguardas adequadas, promova a transparência, integre-se à estrutura geral de governança, responda a incidentes, e seja constantemente atualizado. Essas regras devem ser publicadas, atualizadas periodicamente e podem ser reconhecidas e divulgadas pela autoridade nacional, conforme os incisos §1º e §3º deste mesmo artigo (BRASIL, 2018).

Pinheiro (2020) destaca que as boas práticas “constituem um sistema que institui mecanismos de educação e prevenção envolvendo a segurança da informação, organismos de certificação, treinamento de equipes para cumprimento de regras e atuação com a autoridade nacional”. Além disso, Sankievicz e Pinheiro (2020) relacionam a adoção de uma política de boas práticas e governança como um potencial elemento redutor de eventual penalidade a ser imposta pela autoridade nacional.

Indo para uma análise normativa, conforme estipulado no artigo 50 da LGPD (2018), a lei brasileira estabelece que os controladores e operadores de dados podem formular regras de boas práticas e governança. Essas regras devem considerar a

natureza, o escopo, a finalidade e os riscos e benefícios do tratamento de dados pessoais (2018). A aplicação dos mecanismos de boas práticas, segundo o art. 50. Da LGPD (2018) podem ser implantados por: (i) por meio de associações ou (ii) de forma individual pelo controlador ou operador de dados pessoais.

Ainda em uma análise legal, a LGPD sinaliza que os agentes de tratamento devem estabelecer condições de organização, procedimentos, normas de segurança, obrigações específicas, ações educativas, mecanismos de supervisão e mitigação de riscos, entre outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018)

Segundo Pessoa (2021) a implementação de um programa de compliance de dados apresenta vantagens, como a atenuação de sanções. Ainda a autora, prega pela efetividade da aplicação destes programas, pois se não há a concreta construção de um modelo sustentável e eficiente de compliance, não há em que falar de benefícios. (PESSOA, 2021)

Mencionando outra ferramenta no escopo da boa prática, Sérgio Alves Jr. (2020) ressalta que a implementação de um modelo de ciclo de vida de dados pessoais aderente à LGPD implica que os agentes de tratamento conheçam os dados que estão coletando e armazenando, evitando a coleta e armazenamento irracional e sem critério algum de volumes crescentes de dados pessoais. (JR, 2020)

Continuando a discussão sobre as melhores práticas em um contexto interligado com a figura do encarregado, Saavedra (2020), destaca a conexão entre as etapas do Relatório de Impacto de Proteção de Dados (RIPD) e as melhores práticas de compliance. O relatório, segundo o autor, é uma ferramenta essencial para a prestação de contas, configura-se como um processo meticuloso que delineia o tratamento de dados. Bonna et al. (2022) definem como um processo que tem a função de identificar a necessidade/proporcionalidade, buscando alcançar um equilíbrio harmonioso entre os riscos inerentes a esse tratamento e os direitos que ele confere.

Além disso, Saavedra (2020) ressalta sobre a utilização da ferramenta PbD como uma metodologia essencial para a implementação de um correto tratamento de dados. Este mecanismo implica que as organizações devem sempre criar produtos e serviços que, desde o início, estejam de acordo com as diretrizes de um sistema de

gestão de compliance digital ou de dados, bem como das melhores práticas de Compliance de dados (SAAVEDRA, 2020).

Essas e outras práticas, quando implementadas corretamente, servem como um elemento redutor de eventual penalidade a ser imposta pela autoridade nacional de dados (SANKIEVCZ e PINHEIRO, 2020). Isto é fundamental para o presente artigo, pois se relaciona com a proposta posterior de adentrar nos aspectos específicos de boa prática e governança, seguindo critérios de compliance.

Indo para um conceito de boas práticas pela figura do encarregado, temos o exemplo de orientação para implementação de um Código de Ética e de Conduta, que segundo Saavedra (2020) reflete os valores da empresa e fornece informações sobre o canal de denúncias da empresa. Nesse sentido, o encarregado deve fornecer apropriada orientação para que a implementação deste código seja de acordo também com as outras ferramentas de boas práticas e governança, conforme indicado pelo art. 41. da LGPD. (BRASIL, 2018)

Em suma, o presente tópico abordou a utilização dos mecanismos de boa prática, e também o papel do encarregado nesse contexto. Neste sentido, passamos para o próximo tópico que está indiscutivelmente interligado com a aplicação das boas práticas: as ferramentas de Governança de Dados.

3.4 Governança de dados

A Governança de Dados tem se tornado uma ferramenta essencial para a adequação à LGPD, especialmente no setor público. Segundo Filgueira e Almeida (2020), a governança de dados é o exercício de autoridade e controle sobre o gerenciamento de dados, envolvendo o desenho de políticas e padrões para garantir o uso, segurança, integridade e disponibilidade dos dados. Assim, a governança de dados compreende problemas de ação coletiva e deve ser alicerçada na produção de formas de cooperação para manter a sustentabilidade e resiliência dos dados (MADISON, 2020).

Em uma perspectiva normativa, o Art. 50 da LGPD (BRASIL, 2018), identifica a governança de dados como um conjunto estruturado de regras, políticas e

procedimentos que controladores e operadores de dados devem seguir no tratamento de dados pessoais.

Segundo Tependino Frazão e Oliva (2019) a governança de dados tem um caráter transversal, pois permeia várias estruturas da empresa, não se limitando apenas ao relacionamento com consumidores, mas repercutindo em várias esferas da atividade empresarial. A implementação de um programa de governança de dados requer uma análise abrangente, envolvendo todos os setores da empresa, a parte documental, o objeto e o local das atividades. (PESSOA, 2021)

Silva (2021) ao analisar a aplicação dessa ferramenta pelo setor público, identifica um desafio duplo: garantir o sigilo e a privacidade dos cidadãos e, ao mesmo tempo, garantir um sistema de interoperabilidade que permita o desenvolvimento de políticas públicas eficazes e eficientes

Nesse sentido, a governança de dados se faz necessária, pois a qualidade e a organização das informações são pontos fundamentais para que governos possam planejar políticas públicas eficazes e eficientes, em conformidade com os dispositivos legais, e focadas em atender as demandas dos cidadãos. (MADISON, 2020).

Assim, a reflexão acerca da Governança de Dados ressalta, mais uma vez, a relevância da utilização integrada das ferramentas disponíveis para uma correta adequação, não apenas à legislação brasileira, mas também à implementação de mecanismos padronizados dentro de um processo estrutural de uma organização. Estes últimos podem ser decisivos na prevenção de situações ilegais. Dessa forma, no tópico subsequente, abordaremos um instituto de grande importância para estabelecer os parâmetros de conformidade com a LGPD.

3.5 *Accountability*

A *accountability,* ou prestação de contas, no contexto da proteção de dados, representa uma responsabilidade das organizações em explicar e justificar suas práticas de tratamento de dados pessoais. Esse conceito vai além da mera conformidade com as leis, como a LGPD, exigindo a implementação de medidas eficazes, como políticas claras, avaliação de risco, treinamento, monitoramento e resposta a incidentes. Esse mecanismo promove uma abordagem transparente e

responsável, construindo confiança entre consumidores, funcionários e parceiros de negócios. (MARTINS e GUARIENTO, 2019)

Nesse sentido, é possível relacionar a utilização dessa ferramenta com os princípios basilares da LGPD, pois coaduna com seus conceitos normativos, tanto o princípio da responsabilização e prestação de contas (*Accountability),* quanto do princípio da transparência. (2018). Em seu artigo 6º, X, da LGPD no qual identifica a princípio da responsabilização e prestação de contas, que se define pela “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.” (BRASIL, 2018)

De acordo com a análise de Schedler (1999), a noção de *accountability* pode ser desdobrada em duas dimensões distintas. A primeira, denominada "*answerability*", refere-se à obrigação de informar e justificar ações dentro de um contexto abrangente. A segunda, conhecida como "*enforcement*", está associada à responsabilização ou punição.

Seguindo para a análise de Bovens (2007), a "*answerability*" é um componente da "*accountability*" que se refere à obrigação de informar, explicar e justificar as ações tomadas. Isso é particularmente relevante em instituições públicas, onde os tomadores de decisão devem ser responsáveis perante o público e justificar suas ações. (BOVENS, 2007)

Além disso, a "*answerability*" também é vista como um meio de promover a transparência e a confiança nas instituições. Como apontado por Fox (2015), a essa ferramenta pode servir como um mecanismo para garantir que as instituições sejam transparentes em suas ações e decisões, o que pode, por sua vez, aumentar a confiança do público nessas instituições (FOX, 2015).

De acordo com Behn (2001), a "*answerability*", também é vista como um meio de promover a eficiência e a eficácia nas instituições, podendo incentivar as instituições a serem mais eficientes e eficazes em suas operações, pois a necessidade de justificar suas ações pode levar a uma maior consideração das consequências dessas ações (BEHN, 2001).

Desta dimensão, podemos relacionar com o princípio de prestação de contas da LGPD, pois é segundo o termo de "*answerability*", que o agente de tratamento de

dados, ou aquele que está diretamente envolvido no processo, devendo demonstrar que sua conduta está em conformidade com a lei. (BRASIL, 1988)

Já segundo a dimensão de "*enforcement*", temos uma característica mais punitiva. (1999). Essa é dimensão de accountability que se relaciona com a responsabilização por aquele que violou certa norma (SCHEDLER, 1999).

No estudo de Bovens (2007), enforcement é visto como um mecanismo de controle que visa garantir a conformidade com as normas estabelecidas. O autor argumenta que esta ferramenta é essencial para a eficácia do sistema de *accountability*, pois sem ele, as normas e regulamentos podem ser ignorados sem consequências (BOVENS, 2007).

Talbot (2010) também analisando esta dimensão em sua obra, interpreta que o *enforcement*, possuí um papel crucial no contexto da governança. O autor sugere que esse mecanismo é uma ferramenta crucial para garantir a responsabilidade e a transparência das organizações públicas (TALBOT, 2010).

Ainda relacionado a este mecanismo é possível estabelecer uma ponte ao conceito de responsabilização da LGPD (2018), pois como exposto acima, essa dimensão busca garantir por meio de um controle punitivo, a correta adequação as normas estabelecidas.

Portanto, as dimensões do processo de *accountability* reforçam a sua importância e também a sua conexão com a LGPD. Sendo dois componentes cruciais para utilização de todos os envolvidos no tratamento de dados, no contexto da lei brasileira de proteção de dados.

3.6 Relatório de Impacto à Proteção de Dados (RIPD)

O Relatório de Impacto à Proteção de Dados (RIPD) é mais uma ferramenta crucial que esboça os procedimentos de manipulação de dados pessoais que podem apresentar um alto grau de risco para a observância dos princípios fundamentais de proteção de dados pessoais, tal como delineado na LGPD (2023). Esse mecanismo deve, portanto, abranger as estratégias, precauções e mecanismos de redução de risco, em conformidade com o que é prescrito nos artigos 5º, inciso XVII, e 38 da LGPD. (BRASIL, 2018)

Nos termos dos art. 5º, inciso XVII, e 38, da LGPD (2018)., o RIPD é um instrumento de responsabilidade do controlador, que deve ser realizado antes do início do tratamento de dados pessoais, com uma visão completa de todo o ciclo de vida dos dados (MALDONADO e BLUM, 2019).

Esse relatório deve conter uma explanação detalhada dos variados gêneros de dados adquiridos, bem como a estratégia empregada tanto para a obtenção quanto para a proteção dessas informações. Ademais, é imprescindível que contenha uma avaliação realizada pelo controlador acerca das ações, salvaguardas e mecanismos de redução de risco adotados, tal como estipulado no único parágrafo do Artigo 38 da LGPD. (BRASIL, 2018)

Comparando com outro instituto da GDPR, da União Europeia, o *Data Protection Impact Assessment* (DPIA), podemos analisar que a aplicação do relatório segundo a União Europeia é obrigatória quando o tratamento de dados, especialmente aquele que utiliza novas tecnologias, é suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados, conforme o Art. 35 do GDPR. (UNIÃO EUROPEIA, 2016)

Da mesma forma que o RIPD, a DPIA também estabelece que o documento deve incluir uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos, uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados, e uma avaliação das medidas previstas para enfrentar os riscos. (UNIÃO EUROPEIA , 2016)

A elaboração do RIPD é facultativa na LGPD, diferentemente do DPIA (UNIÃO EUROPEIA, 2016). O órgão regulador de cada país da união, poderá solicitar ao controlador o DPIA, especialmente quando a base legal para o tratamento for o interesse legítimo. As demais situações mandatárias serão dispostas por meio de regulamentação, inclusive quando envolver dados sensíveis

Em suma, o RIPD é uma ferramenta vital para a adequação de todos os envolvidos no tratamento de dados. Este relatório desempenha um papel crucial na garantia de que as organizações não apenas cumpram as suas obrigações legais, mas também adotem uma abordagem proativa e responsável para a proteção de dados. Portanto, a implementação efetiva da RIPD deve ser vista como um

investimento estratégico que pode trazer benefícios a longo prazo para as organizações e para os indivíduos cujos dados elas tratam.

O papel do encarregado na articulação destas ferramentas de proteção de dados torna-se fundamental para a eficácia da governança de dados em conformidade com a lei brasileira, pois, ele atua como um elo integrador entre os diversos princípios e ferramentas, incluindo "Accountability" e "Privacy by Design", garantindo sua implementação coesa e eficaz. Além disso, através da supervisão contínua e da implementação de políticas e procedimentos, o encarregado assegura que a organização esteja em conformidade com as regulamentações legais, promovendo uma cultura organizacional que valoriza a privacidade e a proteção de dados.

A atuação do Encarregado também se estende à promoção da transparência e construção de confiança, servindo como ponto de contato entre a organização, os titulares dos dados e a ANPD. Essa função de comunicação e transparência torna-se precisa no contexto da responsabilização e a boa governança de dados, fortalecendo a relação de confiança com os titulares dos dados e assegurando a conformidade com os princípios legais.

Portanto, a implementação adequada dos princípios de proteção de dados pode mitigar os riscos de violações, influenciando positivamente na avaliação das penalidades. A presença ativa e eficaz de um Encarregado pode ser vista como uma demonstração de boa-fé e diligência por parte da organização, fatores que podem ser considerados na determinação das sanções.

Desta forma, a utilização dessas ferramentas é um elemento-chave para a conformidade com a LGPD. Elas não apenas garantem a proteção dos direitos dos titulares dos dados, mas também previnem possíveis penalidades por não conformidade. Além disso, contribuem para a promoção de uma cultura de respeito à privacidade e à proteção de dados em todos os estratos da organização.

3.7 Responsabilidade no contexto da LGPD

Após a análise das ferramentas utilizadas pelo encarregado, consideradas como boas práticas, é importante abordar os níveis de responsabilidade no contexto da LGPD, para ter como perspectiva como a atuação do encarregado com a utilização

das ferramentas já citadas ao longo deste trabalho, influenciam nas nuances da responsabilização de todos os envolvidos no tratamento de dados.

A responsabilidade civil objetiva é aquela em que o agente é responsável pelo dano causado, independentemente de culpa. No contexto da LGPD, essa responsabilidade pode ser aplicada em casos de tratamento de dados pessoais considerados como atividades de risco. Santos, Leitão e Wolkart (2022)investigam a natureza da responsabilidade civil regulada pela LGPD, analisando se o tratamento de dados pessoais pode ser inserido no rol de atividades de risco, conforme o art. 927, parágrafo único, do Código Civil brasileiro (BRASIL, 2002). A pesquisa sugere uma relação entre a responsabilidade civil prevista na LGPD e a regra de Hand, um critério útil para avaliar a responsabilidade civil dos agentes de tratamento de dados pessoais (SANTOS, MOREIRA, *et al.*, 2023).

A regra de Hand é um critério jurídico formulado pelo magistrado estadunidense Learned Hand, utilizado para avaliar a negligência em casos de responsabilidade civil. Santos, Leitão e Wolkart (2022) investigam o tema da responsabilidade civil por danos decorrentes do tratamento de dados pessoais, nos termos da LGPD, e analisam se a regra de Hand pode ser útil à delimitação da responsabilidade por negligência dos agentes de tratamento de dados pessoais. Os autores, seguinda uma análise compreensiva acerca da LGPD, indicam que a compreensão do juiz Learned Hand pode ser útil à delimitação da responsabilidade civil decorrente do tratamento de dados pessoais (SANTOS, LEITÃO e WOLKART, 2022)

A responsabilidade civil subjetiva, por outro lado, requer a comprovação de culpa, negligência ou dolo por parte do agente causador do dano. No âmbito da LGPD, essa responsabilidade pode ser aplicada em casos específicos, onde a culpa do agente de tratamento de dados deve ser demonstrada. Santos *et al.* (2023) discutem as formas de responsabilidade civil no âmbito da LGPD, destacando que os artigos 42 e 43 da referida lei trazem entendimentos divergentes e abrem possibilidades aos titulares de dados quando do ingresso com demandas no judiciário. O artigo enfatiza a necessidade de entendimentos robustos para que a tutela jurisdicional seja prestada de forma a beneficiar toda a sociedade.

No contexto normativo, o artigo 42 da LGPD (BRASIL, 2018), traz uma série de considerações e possíveis interpretações. O dispositivo menciona uma série de danos

passíveis de reparação, que podem ser patrimoniais, morais, individuais ou coletivos. Este mesmo artigo, não faz referência explícita à culpa, o que poderia sugerir a aplicação de um regime de responsabilidade objetiva. No entanto, a ausência do termo "independentemente de culpa", pode indicar uma inclinação para a responsabilidade subjetiva. Essa omissão na redação do artigo pode ser interpretada como uma escolha deliberada do legislador, refletindo uma preferência pela responsabilidade que depende da avaliação da culpa ou dolo do agente. (SCHREIBER, 2020)

Segundo Araújo (2022), a lei brasileira estabelece um sistema de responsabilidade civil que é considerado especial e proativo, com diversas exigências legais para fins de conformidade. Este sistema reflete o princípio da 'responsabilidade e prestação de contas', que implica na demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Moraes e Peroli (2020), defendem que a responsabilidade seria objetiva, devido à semelhança da estrutura da nova lei com o Código de Defesa do Consumidor e à existência de excludentes de responsabilidade civil que se destinariam ao instituto da responsabilidade objetiva. (ARAÚJO, 2022)

No entanto, Guedes e Meireles (2019) argumentam que o sistema de responsabilidade civil proposto pela LGPD é híbrido e será determinado pela atividade lesante. Araújo (2022), define que em regra, o tipo de responsabilização seria de natureza subjetiva, com a necessidade de comprovação de dolo ou culpa, mas em certas situações, a responsabilidade objetiva seria aplicada, como no caso de danos decorrentes do tratamento de dados pessoais que gerem risco a outrem, realizado pelo Poder Público ou no âmbito das relações de consumo.

Esses conceitos de responsabilidade civil fornecem uma base sólida para a compreensão da culpa normativa, uma forma específica de culpa relacionada ao descumprimento de normas ou regulamentos estabelecidos pela LGPD. A culpa normativa refere-se ao descumprimento de normas ou regulamentos estabelecidos, e no contexto da lei brasileira, essa culpa pode ser atribuída às organizações que falham em cumprir os requisitos da lei.

De acordo com Alves de Lima e Garrido (2022), as organizações contemporâneas enfrentam desafios na adequação às diretrizes da LGPD, tanto em termos de efetividade da lei quanto em questões técnicas e administrativas relacionadas à governança corporativa. A pesquisa aponta para a necessidade de assessoria jurídica customizada às características do negócio como esforço de adequação normativa, evidenciando a complexidade inerente à lei e os desafios para as entidades de direito privado (ALVES DE LIMA e GARRIDO, 2022)

Oliveira (2021) destaca um aspecto fundamental na compreensão da responsabilidade civil do encarregado sob a LGPD. Segundo o autor, tanto a LGPD quanto o GDPR não atribuem responsabilidade direta ao encarregado, mas sim ao controlador e ao operador, conforme estabelecido no Capítulo VI, Seção III da LGPD. (BRASIL, 2018)

Em concordância com Oliveira (2021), é importante observar que a lei brasileira define o encarregado principalmente como um canal de comunicação. Sua função é disseminar boas práticas de proteção de dados dentro da instituição, e ele deve ter a liberdade necessária para cumprir essa função. No entanto, a lei não estabelece requisitos técnicos específicos ou uma área particular de atuação para o Encarregado. Essa falta de especificidade, conforme o autor aponta, significa que o encarregado não precisa ser um administrador da empresa ou um diretor estatutário.

Ainda em uma análise de Oliveira (2021), o autor também aborda a questão da responsabilização pessoal do encarregado. Se caso esse for um administrador e sofrer alguma forma de responsabilização pessoal, isso ocorrerá não por sua função como encarregado, mas por seu papel como administrador. Isso inclui os deveres de obediência, diligência, lealdade, evitar conflitos de interesse e informar. (COMMISSION, 2017)

É possível identificar, que o caminho seguido tanto da LGPD quanto da GPDR, foi de não responsabilizar diretamente o encarregado, mas sobre o Controlador e o Operador. Essa visão alinha-se com as orientações internacionais e oferece uma compreensão sólida da posição do Encarregado dentro da estrutura legal de proteção de dados.

No entanto, mesmo não sendo responsabilizado diretamente pela lei, é plausível analisar que a responsabilidade do encarregado nas organizações é uma

função que transcende a mera conformidade com as regulamentações. O DPO não é apenas um guardião das normas, mas um facilitador que garante que os dados pessoais sejam tratados de acordo com os princípios éticos e legais. Essa responsabilidade, embora complexa, é vital para a integridade e confiança na gestão de informações pessoais.

Transitando para um aspecto ainda mais específico e crítico dessa responsabilidade, a utilização de boas práticas pelo encarregado emerge como um elemento central na prevenção ou atenuação de possíveis autuações por parte da ANPD. Essas boas práticas não são apenas medidas reativas, mas proativas que alinham a organização às expectativas regulatórias, minimizando riscos e fortalecendo a cultura de proteção de dados. A adoção de ferramentas e metodologias adequadas, orientadas por um encarregado, pode transformar a conformidade legal em uma vantagem estratégica, demonstrando comprometimento e transparência. Assim, a função do encarregado torna-se não apenas uma necessidade legal, mas uma parte integrante da governança corporativa, onde a prevenção e a atenuação de sanções são alcançadas através de uma abordagem holística e bem fundamentada.

4 PROCESSO DE DOSIMETRIA DE SANÇÕES ADMINISTRATIVAS NA LGPD

Diante das discussões pregressas, parece viável a explicitação das circunstâncias de fato e de direito que envolvem a dosimetria das sanções administrativas.

A dosimetria das sanções, objeto do capítulo, é um elemento-chave na LGPD, pois estabelece as consequências para os agentes de tratamento que não seguem as diretrizes e requisitos estabelecidos. Assim, o panorama das ferramentas de adequação e conformidade possibilita uma rede de recursos importante para o entendimento das repercussões do papel do Encarregado nesse processo de dosimetria de sanções.

4.1 Parâmetros legais para as sanções administrativas

A ANPD estabelece critérios para determinar as sanções. A magnitude e o método de aplicação dessas penalidades dependem das ações preventivas e corretivas adotadas pelo controlador e operador. Em resumo, se o controlador e o operador, juntamente com o encarregado, tomam medidas suficientes para prevenir ou atenuar as consequências de um vazamento de dados, a penalidade pode ser proporcionalmente menor.

No entanto, se o dano causado pela violação de dados for significativo, as penalidades serão mais severas, conforme a normativa que dispõe que “as sanções serão aplicadas (...) de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso em concreto (...) (BRASIL, 2018).

Ainda segundo a legislação brasileira (BRASIL, 2018), a ANPD na aplicação das penalidades previstas na lei, deve considerar os seguintes parâmetros e critérios:

> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção. (BRASIL, 2018).

Segundo Bonna *et al*. (2022), ao estabelecer esses critérios para as sanções administrativas, a lei brasileira reflete uma tendência internacional de transição de uma abordagem regulatória baseada em comando e controle para uma mais voltada à corregulação e *accountability*. Isso implica que os agentes de tratamento de dados e o Encarregado têm a responsabilidade de adotar medidas eficazes e demonstrar a observância e cumprimento das normas de proteção de dados pessoais. Em outras palavras, a lei incentiva uma postura proativa para garantir a proteção dos dados, ao invés de apenas reagir a possíveis infrações.

No contexto das sanções, Bonna *et al.* (2022) ressalta que a adoção reiterada de mecanismos e procedimentos internos que visam a minimizar danos e a garantir um tratamento seguro e adequado de dados pode ser considerada como critério de dosimetria. Ainda segundo os autores, a implementação de políticas de boas práticas e governança também pode influenciar na determinação das penalidades.

Dessa forma, a atuação do Encarregado pode ser determinante para a efetividade de ferramentas descritas no capítulo anterior no processo de tratamento de dados, na qualidade de profissional que é indicado tanto pelo controlador quanto pelo operador, para comunicação efetiva entre sujeitos interessados e para o comportamento preventivo na cena do tratamento de dados. (BRASIL, 2018).

Outro ponto sobre o qual parece conveniente lançar luzes é a preocupação da legislação em garantir transparência e participação dos interessados na definição dos critérios de sancionamento. A LGPD prevê a elaboração de um regulamento de sanções administrativas, que deve ser submetido a consulta pública, garantindo assim que os critérios sejam claros e conhecidos por todos os envolvidos. (BRASIL, 2018).

Além das tradicionais penas, como advertências e multas, a LGPD introduziu sanções com impactos reputacionais. A possibilidade de "publicização da infração", após sua devida apuração e confirmação, é um exemplo disso. (BRASIL, 2018). Tal medida visa não apenas a penalizar financeiramente o infrator, mas também a alertar a sociedade sobre a infração cometida, o que pode ter decorrências significativas para a imagem e reputação.

Em síntese, o artigo 52 da LGPD estabelece um conjunto de sanções administrativas que refletem uma abordagem equilibrada entre a necessidade de proteger os dados pessoais e garantir que os agentes de tratamento adotem medidas proativas para cumprir a lei.

4.2 O Processo de Dosimetria das Sanções Administrativas na LGPD

A dosimetria das sanções é um processo que busca estabelecer parâmetros e critérios para a aplicação de sanções administrativas pela ANPD, bem como as formas e dosimetrias para o cálculo do valor-base das sanções de multa (BRASIL, 2023).

A LGPD estabelece um conjunto de sanções administrativas que podem ser aplicadas em caso de violações à lei. Essas sanções variam desde advertências até multas que podem chegar a 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração. No entanto, a aplicação dessas sanções deve seguir o princípio da proporcionalidade, levando em consideração a gravidade da infração, a vantagem auferida e a condição econômica do infrator (BRASIL, 2023)

A Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, estabelece que a ANPD pode afastar a metodologia de dosimetria de sanção de multa ou substituir a aplicação de sanção por outra constante no Regulamento, nos casos em que for constatado prejuízo à proporcionalidade entre a gravidade da infração e a intensidade da sanção, conforme exposto no Art. 27 da norma em alusão. Essa decisão deve ser motivada e fundamentada, demonstrando a necessidade e a adequação da medida imposta, a desproporcionalidade constatada, o interesse público a ser protegido e os parâmetros adotados. (BRASIL, 2023).

Além disso, a normativa estabelece critérios para a aplicação de atenuantes e agravantes na dosimetria das sanções. Por exemplo, pode haver uma redução de até 40% na multa se o infrator cooperar com a ANPD durante o processo de fiscalização ou procedimento preparatório que precedeu o processo administrativo sancionador. Por outro lado, a multa pode ser aumentada em até 90% se houver descumprimento de medidas corretivas ou obstrução à atividade de fiscalização (BRASIL, 2023).

É possível perceber, conforme aponta Wimmer (2019), que a LGPD se alinha a uma tendência global, qual seja, a de transformação da lógica regulatória baseada em comando e controle, para a adoção de uma racionalidade que prioriza o enfoque mais voltado para a corregulação e a responsabilização, já definida no dispositivo, chamada de *accountability*. Isso é perceptível em diversos dispositivos da LGPD, que indicam ser responsabilidade do agente de tratamento de dados adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e a eficácia dessas medidas (BRASIL, 2018).

Portanto, é possível identificar que um dos critérios utilizados para a aplicação de sanções é justamente a implementação efetiva de ferramentas que foram expostas nesse presente trabalho, conforme art. 52, § 1.º, VIII (2018). (WIMMER, 2019). Sendo assim, reconhece-se a importância da aplicação de ferramentas que podem auxiliar

não só na prevenção como também na dosimetria das sanções, por parte do Encarregado.

4.3 O Primeiro Caso de Multa por Descumprimento à LGPD

O primeiro caso de multa por descumprimento à LGPD ocorreu em 2023, envolvendo a empresa Telekall Inforservice. Esse caso é de grande importância, pois estabelece um precedente para futuras ações de fiscalização e aplicação de sanções pela ANPD.

O Processo Administrativo Sancionador nº 00261.000489/2022-62 foi instaurado contra a Telekall Inforservice, uma microempresa, em virtude de indícios de transgressão à LGPD. Após a devida apreciação do caso, a ANPD optou por impor à empresa as seguintes penalidades: "Advertência, sem imposição de medidas corretivas, por infração ao art. 41 da LGPD; Multa simples, nos valores de R$ 7.200,00 por infração ao art. 7º da LGPD e de R$ 7.200,00 por infração ao art. 5º do Regulamento de Fiscalização, totalizando R$ 14.400,00". (SANTIAGO, 2023)

A empresa, caso optasse por renunciar expressamente ao direito de recorrer da decisão de primeira instância, seria beneficiada com uma redução de 25% no valor da multa aplicada, desde que efetuasse o pagamento no prazo estipulado pelo Regulamento de Fiscalização.

O episódio envolvendo a Telekall Inforservice, apesar de ser pioneiro em território brasileiro, não se configura como um fenômeno isolado. Globalmente, diversos agentes têm sido penalizados de maneira similar por violações às leis de proteção de dados.

Esses casos internacionais proporcionam ao Brasil uma perspectiva valiosa de compreensão da dosimetria das sações administrativas, pois evidenciam os potenciais consequências do descumprimento da LGPD e ressaltam a importância de uma gestão de dados eficiente.

4.4 O Papel do DPO na Dosimetria de Sanções

O Encarregado atua como um conselheiro, fornecendo orientações e recomendações para o Controlador e o Operador. Sua principal função é monitorar a conformidade com a LGPD, realizar treinamentos para disseminar o conhecimento sobre proteção de dados e servir como um canal de comunicação entre a empresa, os titulares de dados e a Autoridade Nacional de Proteção de Dados (OLIVEIRA, 2021).

A adoção de boas práticas e de governança em privacidade proteção de dados é incentivada pela LGPD e pode influenciar a dosimetria das sanções aplicadas pela ANPD. O papel do Encarregado na dosimetria das sanções administrativa torna-se importante especialmente quando se considera a implementação de ferramentas de boas práticas e governança. Segundo Ryan *et al.* (2021), a figura do Encarregado pode contribuir para monitorar a conformidade a lei, uma vez que cada uma das ferramentas disponíveis de conformidade tem suas limitações. Logo, a depender do grau de zelo do Encarregado e do seu êxito em colaborar para transformar a cultura organizacional, é provável que a dosimetria das sanções leve em conta a responsabilidade, em sentido proativo ou positivo, dos agentes de tratamento.

A implementação de ferramentas de boas práticas e governança, como relatório de impacto de dados, seria uma maneira de otimizar a conformidade com a LGPD. Além disso, a ANPD tem adotado uma abordagem de regulação responsiva, que prioriza a orientação e a educação dos agentes de tratamento de dados, bem como a oportunidade de corrigir não conformidades antes da aplicação de sanções. Isso é evidente na proposta de resolução para a fiscalização e aplicação de sanções pela ANPD, que estabelece uma série de procedimentos para guiar a sua atuação e coloca a aplicação de sanções em segundo plano (OLIVEIRA, 2021).

Portanto, o Encarregado, ao se dispará articular, com a devida técnica profissional, as ferramentas adequadas de boas práticas e de governança em privacidade, desempenha um papel relevante na dosimetria das sanções administrativas, garantindo que as organizações estejam em conformidade com a LGPD e minimizando o risco de sanções. A rigor, a sanção será graduada em proporção inversa ao êxito na implementação de uma cultura organizacional

efetivamente responsável. Por certo, o Encarregado tem muito a colaborar com tal mister.

4.5 A Resolução Cd/Anpd Nº 4, de 24 de Fevereiro de 2023

A Resolução CD/ANPD Nº 4 (BRASIL, 2023) representa um instrumento normativo crucial na estrutura regulatória da proteção de dados no Brasil. Promulgada pela ANPD, essa resolução estabelece diretrizes, parâmetros e procedimentos específicos que complementam e detalham as disposições contidas lei brasileira. A resolução abrange aspectos fundamentais relacionados ao tratamento de dados pessoais, incluindo, mas não se limitando a, definições de obrigações para controladores e operadores, mecanismos de supervisão, critérios para aplicação de sanções e diretrizes para a proteção dos direitos dos titulares dos dados.

A análise e compreensão desta resolução, demonstram sua importância para qualquer entidade envolvida no tratamento de dados pessoais no Brasil, pois serve como um guia interpretativo e operacional para a aplicação efetiva da LGPD. A seguir, serão explorados os principais aspectos e implicações dessa resolução, destacando sua relevância no contexto legal e regulatório da proteção de dados no país.

Art. 7º da Resolução (BRASIL, 2023) estabelece critérios para a definição de sanções em caso de infração à lei brasileira. No inciso I, que trata da gravidade e natureza das infrações, o papel do encarregado é crucial para a implementação de medidas preventivas e corretivas adequadas, garantindo que a organização esteja ciente das possíveis consequências das infrações. O inciso II, referente à boa-fé do infrator, destaca a importância da transparência e cooperação, áreas nas quais o encarregado pode facilitar a demonstração de boa-fé, possivelmente atenuando as sanções.

Nos incisos IX e X, que enfocam a adoção de mecanismos internos e a política de boas práticas e governança, o encarregado pode desempenhar um papel também relevante. Pois, a adoção de mecanismos e procedimentos internos para o tratamento seguro e adequado de dados, bem como a implementação de uma política de boas práticas e governança, são responsabilidades centrais do encarregado. Essas ações

podem minimizar o dano e influenciar positivamente na definição da sanção. (BRASIL, 2023)

O inciso XI, que se refere à pronta adoção de medidas corretivas, enfatiza a necessidade de ação rápida em caso de infração. O encarregado deve estar preparado para implementar prontamente medidas corretivas, o que pode ser considerado na definição da sanção. Essa prontidão reflete a responsabilidade do encarregado em responder eficazmente a qualquer violação, minimizando o impacto sobre os titulares dos dados. (BRASIL, 2023)

Por fim, o inciso XII, que aborda a proporcionalidade entre a gravidade da falta e a intensidade da sanção, ressalta a importância da conformidade total com a LGPD. O encarregado deve trabalhar para garantir que as práticas de tratamento de dados da organização estejam alinhadas com a lei, de modo que qualquer sanção aplicada seja proporcional à gravidade da falta. Essa abordagem equilibrada reforça a importância do encarregado como um pilar central na estrutura de proteção de dados, contribuindo para uma abordagem responsável e transparente ao tratamento de dados pessoais.

O Art. 8º (BRASIL, 2023) classifica as infrações à LGPD em três categorias. Na categoria de infração leve, conforme o inciso I e § 1º, o encarregado deve orientar a organização na prevenção de infrações que não se enquadram nas hipóteses mais graves, mas que ainda podem ter implicações legais e reputacionais. A conscientização e a implementação de medidas preventivas são essenciais para evitar tais infrações.

A infração média, descrita no inciso II e § 2º (BRASIL, 2023), envolve situações que podem afetar significativamente os direitos dos titulares de dados. O encarregado tem a responsabilidade de garantir que as práticas de tratamento de dados não resultem em consequências como discriminação ou fraude financeira. A implementação de medidas de segurança e conformidade adequadas é vital para prevenir infrações dessa natureza.

A categoria de infração grave, conforme o inciso III e § 3º (BRASIL, 2023), inclui várias situações, como tratamento de dados em larga escala, vantagem econômica indevida, e tratamento de dados sensíveis. O encarregado deve estar particularmente atento a essas situações, implementando políticas rigorosas e procedimentos de

controle para evitar infrações graves, que podem resultar em sanções substanciais e danos à reputação da organização.

Por fim, a obstrução à atividade de fiscalização, mencionada no inciso II do § 3º, também é considerada uma infração grave. O encarregado deve facilitar e cooperar com qualquer investigação ou fiscalização, garantindo a conformidade com todas as solicitações e requisitos regulatórios. A transparência e a cooperação nesse aspecto são cruciais para manter a confiança regulatória e evitar sanções adicionais. (BRASIL, 2023)

O Art. 12 (BRASIL, 2023) estabelece as circunstâncias agravantes que podem afetar o valor da multa simples em caso de infração. O inciso I refere-se à reincidência específica, aumentando a multa em 10% para cada caso, até o limite de 40%. O encarregado deve estar ciente dessa circunstância para evitar ações que possam agravar as sanções.

Já o Art. 13 (BRASIL, 2023) estabelece as circunstâncias atenuantes. O inciso II do Art. 13 oferece uma redução de 20% para a implementação de políticas de boas práticas e governança. O encarregado deve garantir que tais políticas estejam em vigor e sejam seguidas, demonstrando o compromisso da organização com a conformidade.

Neste mesmo artigo, o inciso IV do Art. 13 (BRASIL, 2023) identifica uma possível redução de 5% em casos de cooperação ou boa-fé. O encarregado deve promover uma cultura de transparência e cooperação com as autoridades regulatórias, garantindo que essa circunstância atenuante possa ser aplicada. Esses artigos, em conjunto, fornecem um quadro detalhado para o ajuste das multas, e o papel do encarregado pode ser vital, minimizando as sanções através da conformidade proativa e da cooperação.

A Seção XIII desta Resolução (BRASIL, 2023), especificamente o Art. 27, aborda o atendimento ao princípio da proporcionalidade na aplicação de sanções pela ANPD. Este artigo conforme já definido neste presente trabalho, estabelece que a ANPD tem a autoridade para afastar a metodologia de dosimetria de sanção de multa ou substituir a aplicação de sanção por outra, nos casos em que for constatado um desequilíbrio entre a gravidade da infração e a intensidade da sanção.

O princípio da proporcionalidade é fundamental no direito administrativo sancionador, garantindo que as penalidades sejam aplicadas de maneira justa e equilibrada. O Art. 27 reconhece que a metodologia padrão de dosimetria pode, em alguns casos, resultar em sanções que não refletem adequadamente a gravidade da infração. Nesses casos, a ANPD tem a flexibilidade de ajustar a sanção para garantir que ela seja proporcional. (BRASIL, 2023)

A decisão de afastar a metodologia padrão ou substituir a sanção, segundo o mesmo artigo, não pode ser baseada em valores jurídicos abstratos. Deve ser uma decisão motivada e fundamentada, que demonstre claramente a necessidade e adequação da medida imposta. A desproporcionalidade constatada deve ser claramente articulada, e a decisão deve considerar o interesse público a ser protegido e os parâmetros adotados na aplicação da sanção. (BRASIL, 2023)

O papel do encarregado, no contexto deste artigo, é garantir que a organização esteja ciente dessas disposições e trabalhe em conformidade com a lei brasileira. Em caso de procedimento sancionador, o encarregado pode colaborar com a defesa da organização, argumentando sobre a proporcionalidade da sanção, se aplicável, e garantindo que qualquer sanção aplicada esteja em conformidade com os princípios estabelecidos no Art. 27. (BRASIL, 2023)

Em resumo, o Art. 27 fornece um mecanismo importante para garantir que as sanções aplicadas pela ANPD sejam justas e proporcionais à infração cometida. Ele reflete um compromisso com a justiça e a equidade na aplicação da LGPD, permitindo ajustes nas sanções quando necessário, mas exigindo uma fundamentação rigorosa para tais decisões.

Portanto, a Resolução CD/ANPD Nº 4 (BRASIL, 2023), estabelece critérios claros e detalhados para a dosimetria das sanções administrativas em caso de infrações à norma. Essa resolução não apenas delineia as circunstâncias agravantes e atenuantes que podem afetar o valor das multas, mas também enfatiza princípios fundamentais como a proporcionalidade, garantindo que as sanções sejam aplicadas de maneira justa e equilibrada.

Como responsável pela supervisão da conformidade com a LGPD dentro da organização, o encarregado deve estar habituado com essas. Isso inclui compreender

os fatores que podem aumentar ou diminuir as sanções e trabalhar proativamente para implementar políticas e práticas que minimizem o risco de infrações.

Além disso, o encarregado deve estar preparado para agir decisivamente em caso de procedimento sancionador, colaborando com a defesa da organização e garantindo que qualquer sanção aplicada esteja em conformidade com os princípios estabelecidos na resolução. Isso pode incluir argumentar sobre a proporcionalidade da sanção, se aplicável, e trabalhar para implementar medidas corretivas eficazes.

Em conclusão, a Resolução CD/ANPD Nº 4 fornece um quadro abrangente para a aplicação de sanções administrativas sob a LGPD, refletindo um compromisso com a justiça, a transparência e a responsabilidade. O papel do encarregado pode ser vital, garantindo não apenas que a organização cumpra a lei, mas também que responda de maneira eficaz e responsável em caso de infrações.

5 CONCLUSÃO

O encarregado atua como um canal de comunicação entre agentes de tratamento, titulares de dados e ANPD, facilitando o diálogo e a cooperação. A transparência e a colaboração podem ser fatores atenuantes na dosimetria das sanções, refletindo uma postura responsável e proativa.

A figura do Encarregado, diante da possibilidade de utilização das ferramentas citadas acima, pode ter um papel relevante na dosimetria das sanções administrativas da LGPD, haja vista que a sua atuação com a aplicação de ferramentas citadas no trabalho pode otimizar a conformidade com a legislação, e, assim, minimizar o risco de sanções. Logo, nesse rumo, o Encarregado pode atuar como sujeito adjuvante para a construção de uma cultura de proteção de dados no contexto dos agentes de tratamento.

A adoção de boas práticas e governança, conforme Oliveira (2021), são maneiras de demonstrar diligência no tratamento de dados. Tais boas práticas e governança podem traduzir-se em uma série de ferramentas utilizáveis pelo Encarregado para estabelecer um padrão de comportamento responsável para que os agentes pautem a atividade de tratamento de dados.

No inventário dos contributos possíveis, por parte do Encarregado, para a dosimetria, em menor grau, das sanções administrativas, destaca-se a adoção, implementação e elucidação de cláusulas contratuais que favoreçam a robustez da autonomia do titular de dados, assim como de modelos jurídicos que priorizem a boa-fé objetiva e liberdade contratual, enquanto princípios que podem zelar para o equilíbrio relacional e a satisfação de interesses contratuais.

Assim, no contexto da dosimetria, é possível identificar que não se trata de um processo arbitrário, mas sim deum fluxo legalmente formatado para considerar a natureza, a gravidade e a duração da infração, bem como as ações tomadas pelo controlador ou processador para mitigar os danos.

O Encarregado, portanto, desempenha um papel de relevo na demonstração da diligência e do compromisso dos agentes de tratamento com a conformidade. Através da implementação e manutenção de boas práticas, o Encarregado pode fornecer evidências concretas das medidas preventivas e corretivas adotadas. Essas

ações podem ser fundamentais na avaliação da ANPD sobre a aplicação e a extensão das sanções.

Em suma, o encarregado não é apenas um observador passivo no processo de dosimetria das sanções administrativas, mas um participante ativo que pode influenciar o seu resultado através de uma gestão eficaz e ética da proteção de dados. A sua atuação, portanto, vai além da conformidade técnica, abraçando uma visão estratégica que integra a proteção de dados na cultura e na governança da organização, contribuindo para uma abordagem mais equilibrada das sanções.

REFERÊNCIAS

ALFONSIN, T. M. Gestão de Compliance Adequada à Lei Geral de Proteção de Dados na Área da Saúde, Porto Alegre, 2022. Disponivel em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/12166>. Acesso em: 21 jul 2023.

ALMEIDA, G. P. M. D. Proteção de Dados no Contrato de Plano de Saúde: Aspectos Jurídicos da LGPD na Experiência do Consumidor, São Paulo, 2020. Disponivel em: <https://repositorio.pucsp.br/jspui/bitstream/handle/24834/1/Gustavo%20Palheiro%20Mendes%20de%20Almeida.pdf>. Acesso em: 22 jul 2023.

ALMEIDA, V.; FILGUEIRAS, F. **Governance for the digital world:** neither more State nor More Market. London: Springer Nature, 2020. Acesso em: 15 jul 2023.

ALVES DE LIMA, R.; GARRIDO, G. L. Lei Geral de Proteção de Dados (LGPD) e Compliance: Um Panorama da Adequação Normativa para Organizações Contenporâneas., Pouso Alegre, 2022. Disponivel em: <https://periodicos.ufsm.br/revistadireito/article/download/68680/51513>. Acesso em: 07 ago 2023.

ARAÚJO, R. M. F. D. Excludentes de Responsabilidade Civil no Contexto da Proteção de Dados Pessoais. **Tese de mestrado**, São Paulo, 2022. Disponivel em: <https://www.teses.usp.br/teses/disponiveis/2/2131/tde-28092022-105418/publico/11182092MIC.pdf>. Acesso em: 5 ago 2023.

BEHN, R. D. **Rethinking Democratic Accountability**. [S.l.]: Brookings Institution Press, 2001.

BIONI, B. R. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2021.

BONNA, A. P.; , E. A. **Comentários à Lei Geral de Proteção de Dadoss**. Indaiatuba: Foco, 2022.

BOVENS, M. **Analysing and Assessing Accountability:** A Conceptual Framework. European Law Journal: [s.n.], 2007. 447 - 468 p. Disponivel em: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-0386.2007.00378.x>. Acesso em: 11 jul 2023.

BRANCHER, P. M. R. Proteção internacional de dados pessoais. **Enciclopédia Jurídica da PUCSP**, Estrasburgo, 2022. Disponivel em: <https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais>. Acesso em: 15 ago 2023.

BRASIL. Constituição Federal de 1988, Brasília, 1988. Disponivel em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 28 jun 2023.

BRASIL. **Código Civil LEI Nº 10.406**. DF: [s.n.], 2002.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei nº 13.709 de 14/08/2018**, DF, 15 Ago 2018. Disponivel em: <https://normas.leg.br/?urn=urn:lex:br:federal:lei:2018-08-14;13709>. Acesso em: 08 Julho 2023.

BRASIL. Decreto nº 10.474, Brasília/DF, Ago 2020. Acesso em: 21 mai 2023.

BRASIL. Lei nº 14.460 de 25 de Outubro de 2022, Brasília, Out 2022. Disponivel em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14460.htm>. Acesso em: 21 jun 2023.

BRASIL. Resolução CD/ANPD Nº 2, DF, 27 Janeiro 2022. Disponivel em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Acesso em: 12 Jun 2023.

BRASIL. **Guia de Elaboração de Invetário de Dados Pessoais**. 2. ed. Brasília: [s.n.], 2023. Acesso em: 17 ago 2023.

BRASIL. **Resolução CD/ANPD Nº 4**. DF: [s.n.], 2023.

BRUNO, M. G. D. S. SEÇÃO II – Do Encarregado pelo Tratamento de Dados Pessoais. In: BLUM, V. N. M. E. R. O. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: [s.n.], 2019.

CARVALHO, V. M. D.; MATTIUZZO, M.; PONCE, P. P. Boas Práticas e Governaça na LGPD. **Tratado de Proteção de Dados Pessoais**, São Paulo, 2020.

CASCAES, A. C. E. A. **Comentários à Lei Geral de Proteção de Dados à luz do Código de Defesa do Consumidor**. São Paulo: Singular, 2019. Acesso em: 25 jul 2023.

CAVOUKIAN, A. **Privacy by Design:** the 7 Foundational Principles – Implementation and Mapping of Fair Information Practices. [S.l.]: [s.n.], 2013. Disponivel em: <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>. Acesso em: 31 jul 2023.

COMMISSION, E. **Guidelines on Data Protection Officers ('DPOs')**. [S.l.]: [s.n.], 2017. Disponivel em: <https://ec.europa.eu/newsroom/article29/items/612048/en>. Acesso em: 08 ago 2023.

ET AL, A. P. B. **Cometários à leral de proteção de dados pessoais**. Indaiatuba: Foco, 2022.

EUROPEIA, U. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether**. UN. [S.l.]. 2017.

FERNANDES, E.; MEDON, F. Proteção de crianças e adolescentes na LGPD. **Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro**, Rio de Janeiro, 2021. Disponivel em: <https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/download/232/187>. Acesso em: 07 ago 2023.

FERNANDES, M. A. D. S. Repositório Seguro e o Impacto gerado pela lei geral de proteção de dados, Brasília, Set 2022. Acesso em: 18 Jun 2023.

FIGUEIRAS, ; SILVA, B. Assessing Data Policy by Institutional Analysis Development Framework. **International Conference on Public Policy** , Barcelona, 2021. Disponivel em: <https://www.ippapublicpolicy.org/file/paper/60afab524a781.pdf>. Acesso em: 21 jul 2023.

FILHO, E. T. **A Lei Geral de Proteção de Dados Brasileira - Análise Setorial (Volume II).** [S.l.]: Grupo Almedina (Portugal), v. II, 2021.

FONTES, A. C.; LÜTGE, C. Vigilância e Relações de Poder – O Uso de Tecnologias de Reconhecimento Facial e Identificação Biométrica a Distância em Espaço Público e Impactos na Vida Pública, Munich, 2021. Disponivel em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6203/pdf>. Acesso em: 21 jun 2023.

FOX, J. A. Social Accountability: What Does the Evidence Really Say? **American University**, Washington, 2015. Disponivel em: <https://pdf.sciencedirectassets.com/271773/1-s2.0-S0305750X15X00040/1-s2.0-S0305750X15000704/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEHMaCXVzLWVhc3QtMSJHMEUCIQCAUmgAWHVkfuya

b30%2B4KGfELurmu0xxWi8Iyswi1jZwQIgYx%2FUDYyfEHAlsqYkeLDmZDIGDtKWrzngzo5fqt9j>. Acesso em: 21 jul 2023.

GARRIDO, P. P. **Proteção de dados pessoais:** comentários à lei n. 13.709/2018 (LGPD). Belo Horizonte: Editora Saraiva, 2023.

GUEDES, G. S. D. C.; MEIRELES, R. **Término do Tratamento de Dados.** São Paulo: Thomson Reuters Brasil, 2019. p.231 e 233 p.

JR, S. A. Fechando um ciclo: do término do tratamento de dados pessoais (Arts. 15 e 16 da LGPD). **Tratado de Proteção de Dados**, São Paulo, 2020. Acesso em: 21 jun 2023.

KOHLS, C.; DUTRA, L. H.; WELTER,. **LGPD:** da teoria à implementação nas empresas. São Paulo: Rideel, 2021.

LEONARDI, M. Transferência Internacional de Dados Pessoais. **Tratado De Proteção De Dados Pessoais**, São Paulo, 2020. Acesso em: 20 jul 2023.

LIMA, C. R. P. D.; MORAES, E. P. F. D.; PEROLI, K. O Necessário Diálogo entre o Marco Civil da Internet e a Lei Geral de Proteção de Dados para a Coerência do Sistema de Responsabilidade Civil diante das novas tecnologias. In: ROSENVALD, N.; MARTINS, G. M. **Responsabilidade civil e novas tecnologias**. São Paulo: [s.n.], 2020. p. 158-159.

LIMA, J. J. N. D. LGPD e Administração Pública: regulação e aplicação, São Paulo, 2020. Acesso em: 15 jun 2023.

LIRA, B. B. L. D.; MACHADO, D. C. Tratamento e Proteção de Dados no. **LGPD e a Proteção de Dados Pessoais na Sociedade em Rede**, Lisboa, 2022. Acesso em: 12 jul 2023.

LUCAS, L. M. S.; FÉLIX, T. P. Direito Fundamental à proteção de dados e à privacidade na era dos algoritimos e possíveis mecanismos de proteção. **Ponto de Vista Jurídico**, 11, n. 2, 22 jul/dez 2022. p. 84 - 96. Disponivel em: <https://periodicos.uniarp.edu.br/index.php/juridico/article/download/2944/1464>. Acesso em: 15 Junho 2023.

MACHADO, F. I. D. S. Privacidade e Proteção de Dados Pessoais na Sociedade da Informação: profiling e risco de discriminação., Porto Alegre, 2018. Acesso em: 10 Jul 2023.

MADISON, M. J. Tools for Data Governance. **University of Pittsburgh School of Law**, Pittsburgh, 2020. Disponivel em: <https://scholarship.law.pitt.edu/cgi/viewcontent.cgi?article=1393&context=fac_articles>. Acesso em: 21 jul 2023.

MAIMONE, F. H. C. D. P. Responsabilidade Civil na LGPD, Indaiatuba, 2021. Disponivel em: <https://plataforma.bvirtual.com.br>. Acesso em: 18 Jul 2023.

MAIOLINO, E. Z. Representação e responsabilidade política: accountability na democracia, São Paulo, 2015. Disponivel em: <https://bdtd.ibict.br/vufind/Record/USP_ec3bb21671f5aaaff01288c8036531fe>. Acesso em: 12 jul 2023.

MALDONADO, V. N.; BLUM, R. O. **LGPD:** Lei Geral de Proteção de Dados comentada. [S.l.]: Thomson Reuters Brasil, 2019. Acesso em: 10 Jun 2023.
MALUF, G. D. B. Compliance: o que é, quais os tipos e como aplicá-lo na sua empresa? **upLexis**, 2022. Disponivel em: <https://uplexis.com.br/blog/artigos/compliance-o-que-e-quais-os-tipos-e-como-aplica-lo-na-sua-empresa/>. Acesso em: 17 ago 2023.

MARTINS, R. M.; GUARIENTO, D. B. Accountability: a conformidade com o princípio da responsabilização e da prestação de contas. **Migalhas**, 2019. Disponivel em:

<https://www.migalhas.com.br/coluna/impressoes-digitais/315690/accountability--a-conformidade-com-o-principio-da-responsabilizacao-e-da-prestacao-de-contas>. Acesso em: 17 ago 2023.

MULGAN, R. Accountability: An Ever-Expanding Concept? **Public administration**, Canberra, 2000. Disponivel em: <https://crawford.anu.edu.au/pdf/staff/richard_mulgan/MulganR_02.pdf>. Acesso em: 20 jul 2023.

NISSIM, J. Creating a data protection compliance programme. **Data protection: a Pratical guide to UK and EU Law.**, Oxford, 2018. 242. Acesso em: 21 jul 2023.
OLIVEIRA, D. D. L. Agentes de Tratamento de Dados e Encarregado: Guia, SÃO PAULO, 2021.

PESSOA, L. R. D. P. Os Desafios da Governança de Dados e a Realidade Cultural Brasileira, FORTALEZA, 2021. Acesso em: 11 jul 2023.

QUEIROZ, R. C. Z. A proteção de dados pessoais: A LGPD e a disciplina jurídica do Encarregado de Proteção de Dados Pessoais, São Paulo, 2021.

RÊGO, H. D. O. Transparência e Accountability em Portais Brasileiros. **Universidade Federal da Paraíba**, João Pessoa, 2021. Disponivel em: <https://repositorio.ufpb.br/jspui/bitstream/123456789/21446/1/HerbertDeOliveiraR%c3%aago_Tese.pdf>. Acesso em: 21 jul 2023.

RELATÓRIO de Impacto à Proteção de Dados Pessoais (RIPD). **GOV.BR**, 2023. Disponivel em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais/#p1>. Acesso em: 21 jul 2023.

RYAN, P.; CRANE, M.; BRENNAN, R. GDPR Compliance Tools: Best Practice from RegTech, Dublin, 2021. Disponivel em:

<https://doras.dcu.ie/25928/1/Ryan2021_Chapter_GDPRComplianceToolsBestPractic.pdf>. Acesso em: 21 jul 2023.

SAAVEDRA, G. A. Compliance de Dados. **Tratado de proteção de dados**, São Paulo, 2020. Acesso em: 21 jun 2023.

SANKIEVCZ, A.; PINHEIRO, G. P. Aspectos da proteção de dados nas relações de trabalho. **Tratado de proteção de dados**, São Paulo, 2020. Acesso em: 11 jun 2023.

SANTIAGO, A. 1ª empresa é multada no Brasil por violar dados: 'LGPD avança, mas demorou'. - Veja mais em https://www.uol.com.br/tilt/noticias/redacao/2023/07/10/primeira-multa-aplicada-lgpd-brasil.htm?cmpid=copiaecola. **Tilt Uol**, 2023. Disponivel em: <https://www.uol.com.br/tilt/noticias/redacao/2023/07/10/primeira-multa-aplicada-lgpd-brasil.htm>. Acesso em: 17 ago 2023.

SANTOS, R. M. S.; LEITÃO, A. S.; WOLKART, E. N. RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A REGRA DE HAND. **Opinião Jurídica**, 2022. p. 60-84. Acesso em: 9 ago 2023.

SANTOS, V. J. et al. Dano moral - responsabilidade civil na Lei Geral de Proteção de Dados Pessoais (LGPD). **Revista Multidisciplinar da Unisanta Cruz**, 2023. Acesso em: 08 ago 2023.

SARLET, G. B. S.; FERNANDES, M. S.; RUARO, R. L. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. **Tratado de Proteção de Dados Pessoais**, São Paulo, 2020. Acesso em: 20 jul 2023.

SCHEDLER, A. **Self-restraining State:** Power and Accountability in New Democracies. [S.l.]: Lynne Rienner Publishers Inc, 1999.

SCHREIBER, A. Responsabilidade Civil na Lei Geral de Proteção de dados. In: BIONI, B.; OUTROS **Tratado de Proteção de Dados Pessoais**. São Paulo: [s.n.], 2020. Acesso em: 21 jul 2023.

SCHREIBER, A. Responsabilidade Civil na Lei Geral de Proteção de Dados. In: DANILO, D., et al. **Tratado de Proteção de Dados Pessoais**. São Paulo: Forense, 2020. p. 319-338.

SILVA, B. S. D. S. O Impacto da LGPD no Desenho da Política de Governança de Dados nos Municípios: O Caso de Belo Horizonte/MG, Brasília, 2021. Acesso em: 11 jul 2023.

SILVEIRA, A. C. D. M. E. A. **Proteção de dados pessoais na sociedade da informação:** entre dados e danos. Indaiatuba: Foco, 2020. Acesso em: 21 jul 2023.

STEINBERG, R. M. **Governance, Risk Management, and Compliance it Can´t happen to Us-Avoiding Corporate Disaster While Driving Sucess**. [S.l.]: Wiley, 2011.

TALBOT, C. **Theories of Performance:** Organizational and Service Improvement in the Public Domain. [S.l.]: Oxford Press, 2010.

TEIXEIRA, T.; GUERREIRO, R. **Lei Geral de Proteção de Dados Pessoais (LGPD):** Comentada Artigo por Artigo. [S.l.]: Editora Saraiva, 2022.

TEPENDINO, ; FRAZÃO, ; OLIVA, M. D. **A Lei Geral de Proteção de Dados Pessoais e sua Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.

UNIÃO EUROPEIA. **General Data Protection Regulation**. [S.l.]: [s.n.], 2016. Disponivel em: <https://gdpr-info.eu/>. Acesso em: 21 jun 2023.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regula**. [S.l.]: [s.n.], 2016. Disponivel em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1559280280904&uri=CELEX:32016R0679#d1e4683-1-1>. Acesso em: 16 Julho 2023.

VAINZOF, R. Capítulo I. **LGPD: Lei Geral de Proteção de Dados comentada**, São Paulo, 2020. Acesso em: 20 jun 2023.

VALENTE, J. **Promovendo a privacidade e a proteção de dados pela tecnologia:** privacy by design e privacy enhancing-technologies. Rio de Janeiro: Lumen Juris, 2018.

WEBER, K.; OESTERLE, H.; OTTO, B. One Size Does Not Fit All---A Contingency Approach to Data Governance. **ACM Journal of Data and Information Quality**, St. Gallen, 2009. Disponivel em: <https://www.researchgate.net/publication/220177472_One_Size_Does_Not_Fit_All---A_Contingency_Approach_to_Data_Governance>. Acesso em: 17 ago 2023.

WIMMER, M. Os Desafios do Enforcement na LGPD: Fiscalização, Aplicação de Sanções Administrativas e Coordenação Intergovernamental. In: BIONI **Tratado de Proteção de Dados**. São Paulo: Foco, 2019. Cap. 19.